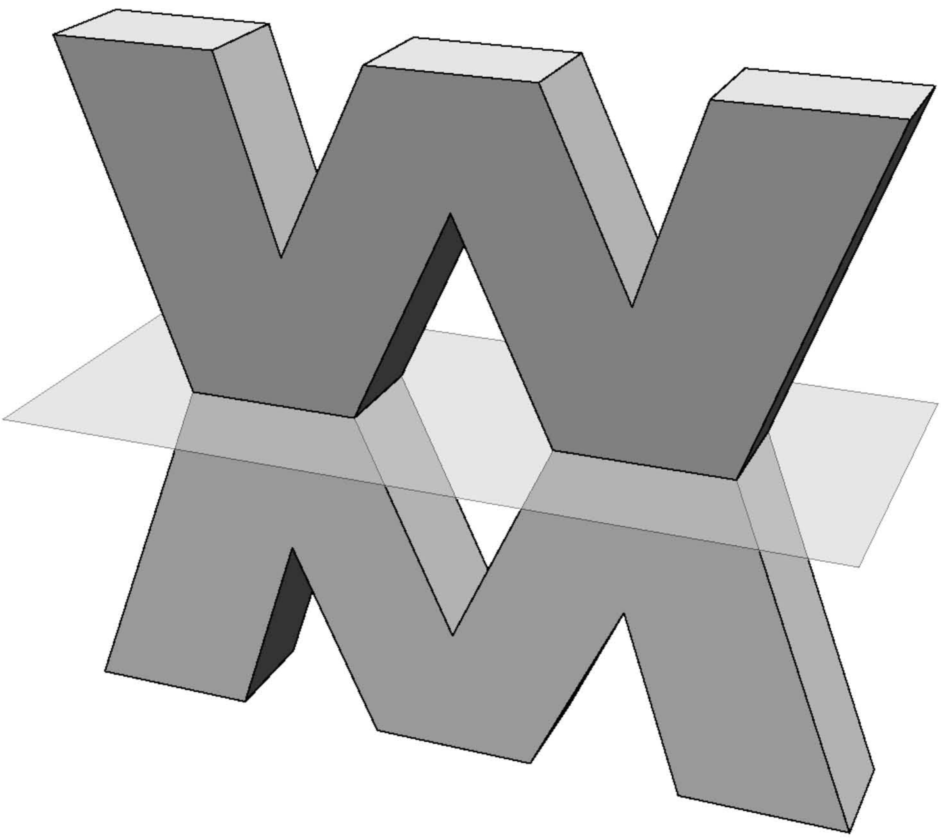
Przemysław Koprowski

Witt Morphisms



Wydawnictwo
Uniwersytetu Śląskiego
Katowice 2012

Witt morphisms

PRACE NAUKOWE
UNIWERSYTETU
ŚLĄSKIEGO
W KATOWICACH

NR 2966

Przemysław Koprowski

Witt morphisms

Wydawnictwo Uniwersytetu Śląskiego Katowice 2012

Redaktor serii: Matematyka
Tomasz Dłotko

Recenzent
Grzegorz Banaszak

Publikacja będzie dostępna — po wyczerpaniu nakładu — w wersji internetowej:

Śląska Biblioteka Cyfrowa
www.sbc.org.pl

Contents

Foreword

A bilinear form defines an orthogonal geometry on a given linear space or projective module. Once we omit degenerate forms (roughly speaking, these are forms allowing a non-zero vector to be orthogonal to the entire space), the remaining ones may be classified by the relation of similarity (the term is explained in Section 1.1). This leads us to the notion of the Witt ring, which is an algebraic structure consisting of all the similarity classes of finitely generated projective modules over a given base ring. In a sense, Witt ring describes all the possible orthogonal geometries over the ring/filed in question. The leading theme of this book is to study morphisms between Witt rings. In geometric terms, this can be viewed as analyzing to what extent the orthogonal geometries defined over one ring may be transcribed to another ring. For example, knowing the criteria for existence of an isomorphism between Witt rings, one may verify whether two rings/fields admit the same set of orthogonal geometries. If this is the case we say that the two rings are *Witt equivalent*. This problem has been intensively researched in previous years. The complete criteria are known for fields with small square class groups (see [9]) and global fields (see e.g. [44, 53, 52]). The author of this book found criteria for Witt equivalence of function fields and rings of regular function on real algebraic curves (summary of these results can be found in the appendix to Chapter 5). The criterion of Witt equivalence of real function fields has been recently generalized by N. Grenier-Boley and D. Hoffmann to arbitrary real fields with u-invariants not exceeding 2. We present their result in Section 5.1. In the second section of the last chapter we apply the ideas used earlier for rings of regular function on real curves to extend the result of Grenier-Boley and Hoffmann and obtain a necessary condition (see Theorem 5.15) for Witt equivalence of real holomorphy rings. This generalizes our earlier result obtained in [27].

Chapter 4 copes with a splitting of the Knebusch-Milnor exact sequence. A classical theorem due to M. Knebusch and J. Milnor (see Theorem 1.40) assert that the Witt ring WR of a Dedekind domain R injects into the Witt ring of its field of fractions K and the image of this embedding coincides with the kernel of a map from the Witt ring of the field to the co-product of Witt rings of all the localizations of the base ring. In a nutshell, this says that the structure of orthogonal geometries over K is at least as rich as the structure over the underlying Dedekind domain. Surprisingly, not much is known about the splitting of the above-mentioned injection $WR \rightarrowtail WK$. The problem was solved in the case of algebraic integers by P. Shastri in [50] and for real geometric rings by the author in [26] and [28]. Chapter 4 summarizes the results of these two papers. The main result of this chapter (see Theorem 4.3) asserts that, if R is the ring of regular functions on a smooth real curve, then WR is a direct summand of the Witt ring of the field of fractions of R (the field of rational functions on this curve). Consequently, the Knebusch-Milnor exact sequence slices into and is patched by two split exact sequences (c.f. Theorem 4.17). Moreover, if the curve in question is semi-algebraically compact and semi-algebraically connected, then the Witt ring of the ring of polynomial function is in turn a direct summand of WR as shown in Theorem 4.19.

On the other hand, it is natural to reckon that starting from a ring with a complex Witt ring (i.e. with a rich structure of orthogonal geometries) and appending roots of (quadratic) polynomials one can successively kill elements of the Witt ring. Therefore, it is expected that the natural morphism of Witt rings corresponding to an algebraic (resp.: real, quadratic or integral) closure of a field/ring should *not* be injective. A classical example: start from the field $\mathbb{Q}$ of rationals, let R denote its real closure and $R[\sqrt{-1}]$ be the algebraic closure. The Witt ring of $\mathbb{Q}$ has quite a complex structure (as additive group it is a direct sum of infinitely many nontrivial term, see [33, Chapter VI, Section 4]), while WR is isomorphic to the ring of integers and $WR[\sqrt{-1}]$ consists of just two elements. Thus, the injections $\mathbb{Q} \rightarrowtail R \rightarrowtail R[\sqrt{-1}]$ correspond to the maps $W\mathbb{Q} \to WR \to WR[\sqrt{-1}]$, both having strongly nontrivial kernels. In Chapter 3 we concentrate on an analogy of this phenomenon in the case of the integral closure of a ring. For example, we show (see Theorem 3.15) that if P is seminormal but not quadratically closed and R is the integral closure of P, then the natural morphism $WP \to WR$ is not injective. This problem has also a natural interpretation in terms of the Picard functor. This connection is studied in Section 3.3. We close this chapter showing how to apply these results in the case of curve desingularization.

The Witt functor of a ring extension is also the subject of the second chapter. Here, however, we consider a quadratic extension of a local ring. We develop a generalization of Scharlau's transfer and prove an analogy of Scharlau's norm principle. This allows us to construct examples of ring extensions where both rings have the same field of fractions but the corresponding Witt morphism is not surjective (hence there are classes of forms over the bigger ring not comming from the smaller one).

The new contributions in this book include: entire Chapters 2 and 3 and Section 5.2 where the main new results are Theorems: 2.17, 2.19, 2.24, 3.11, 3.15, 3.24, 5.15 and Proposition 2.35. The results of Chapter 4 appeared earlier in

[26, 28]. The proofs presented here are only slightly improved and unified to better fit together. The results gathered in the appendix to Chapter 5 were published in [24, 25, 27, 29]. All the theorems of Chapter 1 are classical and well known. The intend of the author was to make the book as self-contained as possible, to save the reader from the need to refer to any external sources while reading. Hence the opening chapter contains a basic introduction to the theory of bilinear forms, valuations and orderings, serving as a handy reference for the following chapters. The presentation of the first chapter is necessarily brief and most of the proofs are omitted.

A short remark on the notational convention. We tend to use letters P and R to denote rings. While the latter is widely used and self-explaining (as the first letter of the word "ring"), the use of P requires some justification. We often need to compare two rings and so R alone is not enough. The letter P is close enough to R so that we can write "P is a subring of R" with the inclusion relation preserving the natural alphabetical order. Secondly, P is the first letter of the Polish word "pierścień" (which means ring), hence we have P for "pierścień" and R for "ring". The rest of notation used in this book is standard and agrees with broadly accepted conventions. For reader's convenience, we include the list of commonly used symbols on page 89.

1

Preliminaries

The aim of this chapter is to provide the reader with a condensed account of basic theory of bilinear forms, orderings and real curves, which is needed in the rest of these notes. This serves a double purpose of establishing the notation we use in the last two chapters and provide a handy reference for the results we use. The presentation is rather brief, since otherwise a detailed exposition of such a wide range of topics would require a monograph of at least ten times the size of this book. In particular, we restrict ourselves only to the results which are utilized later. This of course does not mean that the topics left out are unimportant or uninteresting. Moreover, in order to sustain a reasonable length of this chapter we omit the proofs except in Section 1.3.

1.1. Witt functor

In these notes, the term *ring* will always mean a commutative ring with unity. The symbol UP denotes the group of invertible elements of a ring P and $\dot{P}$ is the set of all the elements of P that are not zero divisors. Of course, over a field K, one has $UK = \dot{K}$. In this case we will prefer the later symbol.

Definition 1.1. Let P be a ring such that $2 \in UP$ and let M be a finitely generated projective module over P. A (*symmetric*) *bilinear form* on M is a map $\xi : M \times M \to P$ satisfying the conditions

- $\xi(x, y) = \xi(y, x)$ for all $x, y \in M$;
- $\xi(ax + by, z) = a\xi(x, z) + b\xi(y, z)$ for all $a, b \in P$ and $x, y, z \in M$.

Later we will usually drop the adjective "symmetric", or even sometimes use just the term "form" alone, to mean a symmetric bilinear form. This should not lead to any confusion since we do not make any reference to non-symmetric forms neither to the forms of other degrees. Observe that we define bilinear forms (and consequently the derived objects like Witt rings)

exclusively over rings in which 2 *is invertible.*

This is a global assumption valid throughout this whole book. For a function $f : X \to Y$ having some domain X and a codomain Y, it is a common practice to abbreviate the notation and write f alone. Likewise, having a known base-ring P we shall often say "ξ is a bilinear form over P" to mean that ξ is actually defined on some finitely generated projective module over P. If the module is important, we will write a pair (M, ξ) and refer to it as a *bilinear module*.

DEFINITION 1.2. A bilinear module (M, ξ) is *non-degenerate* if the adjoint homomorphism $\hat{\xi} : M \to \operatorname{Hom}_P(M, P)$, $\big(\hat{\xi}(x)\big)(y) := \xi(x, y)$ is an isomorphism.

If the base ring is actually a field K, then a f.g. module is simply a finitely dimensional vector space. Then a form ξ on a space V is non-degenerate, if and only if the null vector is the only one orthogonal to the whole space, i.e. $\xi(v, w) = 0$ for all $w \in V$ implies that $v = \Theta_V$.

With every bilinear form ξ we associate a *quadratic form* q defined as $q(x) := \xi(x, x)$. The bilinear form ξ may be recovered from q by the formula

$$\xi(x, y) = \frac{1}{2}\big(q(x + y) - q(x) - q(y)\big).$$

The bilinear and quadratic forms are thus in one-to-one correspondence and we shall pass from one to the other when it is convenient.

Two non-degenerate bilinear modules (M, ξ), (N, ζ) are *isometric*, if there is a P-module isomorphism $\varphi : M \xrightarrow{\sim} N$ such that $\xi(x, y) = \zeta(\varphi(x), \varphi(y))$ for all $x, y \in M$. We then write $(M, \xi) \cong (N, \zeta)$. If (M, ξ) and (N, ζ) are two non-degenerate bilinear modules one may define non-degenerate forms on their direct sum $M \oplus N$ and the tensor product[1] $M \otimes N$ (see [36, Chapter 1, §3]). The first is given by the formula

$$(\xi \perp \zeta)(x \oplus y, z \oplus t) := \xi(x, z) + \zeta(y, t),$$

while the later is defined on simple tensors by

$$(\xi \otimes \zeta)(x \otimes y, z \otimes t) := \xi(x, z)\zeta(y, t)$$

and extended to $M \otimes N$ by linearity. The forms $\xi \perp \zeta$ and $\xi \otimes \zeta$ are called the *orthogonal sum* and the *tensor product* of ξ, ζ. These two operations are associative, commutative and preserved by an isometry. Moreover $\otimes$ is distributive over $\perp$. For a subset $S \subseteq M$ of a bilinear module (M, ξ) we denote $S^\perp := \{x \in M : \xi(x, S) \equiv 0\}$.

PROPOSITION 1.3. *Let (M, ξ) be a non-degenerate bilinear module. The following conditions are equivalent:*

- *there is a direct summand N of M such that $N = N^\perp$;*
- *$M = N \oplus N'$ with $\xi(N, N) \equiv 0$ and $\hat{\xi}(N) = \operatorname{Hom}_P(N', P)$;*
- *$M = N \oplus N'$ with $\xi(N, N) \equiv 0$ and $\hat{\xi}(N) = \operatorname{Hom}_P(N', P)$ and also $\hat{\xi}(N') = \operatorname{Hom}_P(N, P)$;*

[1] An unadorned tensor product means a tensor product over the base ring P.

- $M = N \oplus N'$ *with* $\xi(N, N) \equiv 0$, $\xi(N', N') \equiv 0$, $\hat{\xi}(N) = \operatorname{Hom}_P(N', P)$ *and* $\hat{\xi}(N') = \operatorname{Hom}_P(N, P)$*;*

For the proof we refer the reader to [39, Chapter 1, §6]. A bilinear module is *hyperbolic* if it satisfies any (hence all) of the conditions of the previous proposition. If P is a domain (more generally, if P does not contain any idempotents other than 0 and 1), then every module over P has a constant rank (see e.g. [48, Corollary 2.12.23]). Suppose that M is a free module of rank k over P, a bilinear form ξ on M can be written (see [39, Chapter 1, §2]) as

$$\xi\Bigl(\begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix}, \begin{pmatrix} y_1 \\ \vdots \\ y_k \end{pmatrix}\Bigr) = (x_1, \dots, x_k) \cdot \Xi(\xi, \mathscr{B}) \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_k \end{pmatrix},$$

where $(x_1, \dots, x_k)$ and $(u_1, \dots, y_k)$ are the coordinates of elements of M with respect to some fixed basis $\mathscr{B}$ and $\Xi(\xi, \mathscr{B})$ is a $k \times k$ matrix with entries in P. The determinant of the matrix $\Xi(\xi, \mathscr{B})$ is independent of the choice of the basis $\mathscr{B}$, hence it is an invariant of the isometry class of ξ. We denote it $\det \xi$. However, a more convenient invariant is the *discriminant* $\operatorname{disc} \xi$ defined by $\operatorname{disc} \xi := (-1)^{k(k-1)/2} \det \xi$.

Proposition 1.4 ([39, Lemma I.2.2]). *The form ξ is non-degenerate if and only if the matrix $\Xi(\xi, \mathscr{B})$ is invertible.*

In a special case, if the basis $\mathscr{B}$ is orthogonal, then $\Xi(\xi, \mathscr{B})$ is a diagonal matrix with some entries $u_1, \dots, u_k$. We will shortly write then $\xi \cong \langle u_1, \dots, u_k \rangle$ and call it the *diagonalization* of ξ.

Corollary 1.5. *The form $\langle u_1, \dots, u_k \rangle$ is non-degenerate iff all u_i's are invertible.*

For $u_1, \dots, u_k \in UP$, the tensor product $\langle 1, u_1 \rangle \otimes \cdots \otimes \langle 1, u_k \rangle$ is called a *k-fold Pfister form* and shortly denoted $\langle\langle u_1, \dots, u_k \rangle\rangle$. Recall that a ring is *local* if it contains exactly one maximal ideal, it is *semi-local* if it has finitely many maximal ideals.

Proposition 1.6 ([34, Theorem X.4.4]). *Every finitely generated projective module over a semi-local ring is free.*

Proposition 1.7 ([36, Proposition II.2.3]). *Over a semi-local ring every non-degenerate bilinear form is diagonalizable.*

Proposition 1.8 ([39, Lemma I.6.3]). *Let P be a ring such that every finitely generated projective P-module is free (e.g. P is semi-local). If (M, ξ) is a hyperbolic bilinear module over P, then it has a basis $\mathscr{B}$ such that the associated matrix is*

$$\Xi(\xi, \mathscr{B}) = \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}.$$

Definition 1.9. Let (M, ξ) be a non-degenerate bilinear module over P. An element $x \in M$ is *strongly isotropic* if $\xi(x,x) = 0$. It is *weakly isotropic* if $\xi(x,x) \notin UP$.

In these notes we will often need to consider bilinear modules of the form $I \oplus P^n$, where P is a Noetherian ring of dimension one (i.e. every non-zero prime ideal of P is maximal) and $I \lhd P$ is a suitably chosen ideal. The following results determine the structure of a bilinear form over such a module. Recall that a *line bundle* is a f.g. projective module of rank 1. In propositions 1.10–1.15 P is always a Noetherian domain of dimension one.

Proposition 1.10 ([32, Corollary (2.21)]). *Every line bundle over P is isomorphic to an invertible fractional ideal of P and every invertible fractional ideal is a line bundle.*

Proposition 1.11 ([15, § 11.3]). *Every finitely generated fractional ideal of P is isomorphic as a P-module to an (ordinary) ideal of P.*

Proposition 1.12 ([30, Chapter IV, §3]). *A finitely generated projective P-module M of rank n is isomorphic to a module $I \oplus P^{n-1}$ for some ideal I of P.*

Proposition 1.13 ([11, Theorem 2.6]). *A projective module $I \oplus P^n$ where $I \lhd P$ admits a non-degenerate bilinear form if and only if I^2 is principal.*

Proposition 1.14 ([45, Proposition 2.8]). *Let $I \oplus P^n$ be a projective P-module, where $I \lhd P$ is an ideal such that $I^2 = d \cdot P$ for some element $d \in P$. Any bilinear form $\xi : (I \oplus P^n) \times (I \oplus P^n) \to P$ on $I \oplus P^n$ is given by a formula:*

$$\xi\left(\begin{pmatrix} x \\ y_1 \\ \vdots \\ y_n \end{pmatrix}, \begin{pmatrix} x' \\ y_1' \\ \vdots \\ y_n' \end{pmatrix}\right) = \frac{1}{d}(x, y_1, \ldots, y_n) \left(\begin{array}{c|ccc} a & b_1 & \cdots & b_n \\ \hline b_1 & c_{11} & \cdots & c_{1n} \\ \vdots & \vdots & & \vdots \\ b_n & c_{1n} & \cdots & c_{nn} \end{array}\right) \begin{pmatrix} x' \\ y_1' \\ \vdots \\ y_n' \end{pmatrix}$$

for some $a \in UP$, $b_i \in I$ $(1 \le i \le n)$ and $c_{ij} \in I^2$ $(1 \le i, j \le n)$.

Proposition 1.15 ([45, Theorem 2.9]). *The form ξ of the previous proposition is non-degenerate if and only if the determinant of the above matrix satisfies the condition:*

$$\det \begin{pmatrix} a & b_1 & \cdots & b_n \\ b_1 & c_{11} & \cdots & c_{1n} \\ \vdots & \vdots & & \vdots \\ b_n & c_{1n} & \cdots & c_{nn} \end{pmatrix} = ud^n$$

for some unit $u \in UP$.

Definition 1.16. Two bilinear modules (M, ξ), (N, ζ) are called *similar* if there are hyperbolic bilinear modules (M', ξ') and (N', ζ') such that $(M, \xi) \perp (M', \xi') \cong (N, \xi) \perp (N', \zeta')$.

The similarity is an equivalence relation and preserves orthogonal sums and tensor products. The equivalence class of a form ξ is called the *Witt class* of ξ. Abusing the notation slightly, we denote it ξ again.

THEOREM 1.17 ([39, Theorem I.7.3]). *The set of Witt classes of non-degenerate symmetric bilinear forms over a given ring P forms a ring with operations induced by the orthogonal sum and the tensor product.*

The ring described by the above theorem is called the *Witt ring* of P and denoted WP. In some cases, we are interested only in the additive structure of WP. To emphasize this point of view, we refer to the additive group of WP as to the *Witt group* of P. If $\varphi : P \to R$ is a ring homomorphism, then φ induces a ring homomorphism $WP \to WR$ mapping the Witt class of a bilinear module (M, ξ) to the Witt class of $M \otimes R$ with a bilinear form $(x \otimes a, y \otimes b) \mapsto ab\varphi\bigl(\xi(x, y)\bigr)$ (c.f. [39, Theorem I.5.4]). In particular, assigning the Witt ring WP to a ring P, one defines a functor from the category of commutative rings with 2 invertible[2] to the category of commutative rings. We call it the *Witt functor* and for a ring morphism $\varphi : P \to R$ we denote the associated morphism of Witt rings by $W\varphi$.

Remark 1.18. A bilinear form ξ defines an orthogonal geometry on a P-module, with two vectors x, y being orthogonal once $\xi(x, y)$ is zero. Thus, in a certain sense, the Witt ring gathers information about all the possible orthogonal geometries over a given base ring. Consequently, Witt functor $W\varphi$ of a ring homomorphism $\varphi : P \to R$ tells us, to what extent orthogonal geometries defined over P are carried over to R. The most natural case is the canonical inclusion $P \rightarrowtail R$ of some ring extension $P \subset R$. If $W(P \rightarrowtail R)$ is injective, then it means that the structure of orthogonal geometries over R is at least as rich as that over P. We deal with this question in Section 1.3 and later in Chapters 3 and 4.

1.2. Orderings and valuations

In this section we gather basic information about orderings, valuations and their compatibility. As in other sections of this chapter, we omit the proofs and restrict ourselves only to this (very limited) part of the theory which is needed in the rest of this book. This section is based mostly on the books [31, 36, 37] to which we refer the reader for a more complete exposition.

DEFINITION 1.19. Let P be an integral domain. An *ordering* of P is a multiplicatively and additively closed subset $\beta \subset P$ such that $\beta \cup -\beta = P$ and $\beta \cap -\beta$ is a prime ideal, called the *support* of β.

[2] One can also define the Witt ring of a ring in which 2 is not invertible. The assignment $P \mapsto WP$ is still a functor, then.

We say that an element $x \in P$ is positive with respect to β if $x \in \beta$. If the domain we deal with is actually a field, then the only prime ideal is $\{0\}$. It follows that a subset β of a field K is an ordering if and only if $\beta+\beta, \beta\cdot\beta \subseteq \beta$, $\beta\cup-\beta = K$ and $\beta\cap-\beta = \{0\}$. The space of orderings of a field K is denoted $\mathcal{X}_K$. Over a field, an ordering β defines a relation $\leq_\beta$ by the condition $x \leq_\beta y \iff y - x \in \beta$. It is straightforward to check that $\leq_\beta$ is a total order compatible with the addition and the multiplication in the sense that $x \leq_\beta y$ implies $x + z \leq_\beta y + z$ and $0 \leq_\beta x, y$ implies $0 \leq_\beta xy$ for every $x, y, z \in K$. Conversely, every total order $\preceq$ on K which is compatible with the addition and the multiplication induces an ordering β of K such that $\leq_\beta$ coincides with $\preceq$ (see e.g. [5, §1.1]).

Proposition 1.20 ([37, Proposition 5.1.1]).

1. *Orderings of an integral domain P with the support $\{0\}$ are in one-to-one correspondence with orderings of its field of fractions* $\operatorname{qf}(P)$.
2. *Any ordering β of P with the support $\mathfrak{p}$ induces an ordering on the residue field* $\operatorname{qf}(P/\mathfrak{p})$.
3. *For any prime ideal $\mathfrak{p} \in \operatorname{Spec} P$, every ordering $\overline{\beta}$ of $\operatorname{qf}(P/\mathfrak{p})$ lifts to an ordering β of P with the support $\mathfrak{p}$.*

Observation 1.21. *Let β be an ordering of a ring P, then*

1. $\sum P^2 \subseteq \beta$;
2. $-1 \notin \beta$.

Proof. For every $a \in P$ either $a \in \beta$ or $-a \in \beta$, it follows that $a^2 \in \beta$. Now, an ordering is additively closed, hence $\sum P^2 \subseteq \beta$, which proves (1.21). To prove (1.21), observe that $1 = 1^2 \in \beta$, so if $-1 \in \beta$ it would follow that $1 \in \beta \cap -\beta$ which is impossible since the support of an ordering is a prime ideal. □

It follows immediately from the above observation that the only fields that can possibly admit an ordering are those of characteristic zero. The theory of ordered fields earned its position in the modern algebra mostly due to the following celebrated theorem of E. Artin and O. Schreier.

Artin–Schreier Theorem 1.22 ([33, Theorem VIII.1.10]). *A field K admits at least one ordering if and only if -1 is not a sum of squares in K*

A field K with $-1 \notin \sum \dot{K}^2$ is said to be *formally real.* A formally real field having no proper formally real extensions is called *real closed.* The field $\mathbb{R}$ of reals is a basic example of a real closed field. In a real closed field K every sum of squares is actually a square and the set of squares (together with zero) constitutes the unique ordering of K.

Proposition 1.23 ([33, Theorem VIII.2.8]). *If K is a field together with an ordering β, then there is a real closed field L such that L/K is an algebraic extension and $\beta = K \cap L^2$.*

Artin Theorem 1.24 ([33, Theorem VIII.1.12]). *A non-zero element of a formally real field is totally positive (i.e. positive with respect to every ordering $\beta \in \mathcal{X}_K$) if and only if it is a sum of squares.*

We shall now briefly report on a connection between orderings and (real) valuations of a field.

Definition 1.25. Let K be a field, a subring $\mathcal{O} \subset K$ such that for every $x \in K$, either $x \in \mathcal{O}$ or $x^{-1} \in \mathcal{O}$ is called a *valuation ring* in K.

Obviously K itself is a valuation ring. It is a *trivial* valuation ring. Every valuation ring is a local domain (see e.g. [17, Corollary 6.4]) with the maximal ideal $\mathfrak{m} = \{x \in \mathcal{O} : x^{-1} \notin \mathcal{O}\}$.

Definition 1.26. Let K be a field and Γ a totally ordered abelian group. A (*Krull*) *valuation* on K is a mapping $v : K \twoheadrightarrow \Gamma \cup \{\infty\}$ satisfying the following conditions:

1. $v(x) = \infty \iff x = 0$ for every $x \in K$;
2. $v(xy) = v(x) + v(y)$ for all $x, y \in K$;
3. $v(x + y) \geq \min\{v(x), v(y)\}$ for all $x, y \in K$.

Two valuations $v_1 : K \twoheadrightarrow \Gamma_1 \cup \{\infty\}$, $v_2 : K \twoheadrightarrow \Gamma_2 \cup \{\infty\}$ are *equivalent* if there is an order-preserving isomorphism $\varphi : \Gamma_1 \xrightarrow{\sim} \Gamma_2$ such that $v_2 = \varphi \circ v_1$. If $v : K \twoheadrightarrow \Gamma$ is a valuation, then $\mathcal{O}_v := \{x \in K : v(x) \geq 0\}$ is a valuation ring of K. In fact, the mapping $v \mapsto \mathcal{O}_v$ determines a bijection between equivalence classes of valuations of K and valuation rings in K (see e.g. [17, Theorem 7.1]). The field $K(v) := \mathcal{O}_v/\mathfrak{m}$ is called the *residue field* of v. A valuation v is called *real*, respectively a valuation ring is called *residually real*, if the residue field $K(v)$ is formally real.

Definition 1.27. An ordering $\beta \in \mathcal{X}_K$ and a valuation v of a field K are said to be *compatible* if any (hence all) of the following equivalent conditions holds (c.f. [31, Theorem 2.3])

1. $0 <_\beta x \leq_\beta y$ implies $v(x) \geq v(y)$;
2. if $x \in \beta$ and $v(x) < v(y)$, then $x >_\beta y$;
3. $1 + \mathfrak{m} \subset \beta$.

We say that a valuation $v : K \twoheadrightarrow \Gamma \cup \{\infty\}$ is *discrete of rank* 1, if $\Gamma \cong \mathbb{Z}$ (as ordered groups). If this is the case, then the associated valuation ring is a principal ideal domain. A *uniformizer* of v is then a generator p of the maximal ideal $\mathfrak{m}$

of $\mathcal{O}_v$. Any non-zero element $x \in K$ can be written uniquely in the form $x = up^n$ for some $n \in \mathbb{Z}$ and $u \in U\mathcal{O}_v$. It follows that $v(x) = n$. In what follows, we will often consider discrete rank 1 valuations $K \twoheadrightarrow \mathbb{Z} \cup \{\infty\}$, where K is a field of fractions of a given ring P, and the valuation ring is a localization of P at some prime ideal $\mathfrak{p}$. In such cases, we use the following notation: we write $(\mathcal{O}_\mathfrak{p}, \mathfrak{p})$ for the valuation ring; next, $\operatorname{ord}_\mathfrak{p}$ denotes the valuation and $K(\mathfrak{p}) := \mathcal{O}_\mathfrak{p}/\mathfrak{p}$ is the residue field. The residue class of a unit $u \in U\mathcal{O}_\mathfrak{p}$ is denoted by $u(\mathfrak{p})$. A discreet rank 1 valuation $\operatorname{ord}_\mathfrak{p} : K \twoheadrightarrow \mathbb{Z} \cup \{\infty\}$ defines an absolute value $|\cdot|_\mathfrak{p}$ on K by the formula $|x|_\mathfrak{p} := 2^{-\operatorname{ord}_\mathfrak{p} x}$. A field is *complete* if every Cauchy sequence in K converges.

THEOREM 1.28 ([17, Theorem 3.2]). *If* $\operatorname{ord}_\mathfrak{p}$ *is a discrete rank* 1 *valuation on* K*, then there is a field extension* $K \subseteq K_\mathfrak{p}$ *with* $K_\mathfrak{p}$ *complete and* K *dense in* $K_\mathfrak{p}$*.*

LEMMA 1.29. *Let* $\operatorname{ord}_\mathfrak{p}$ *be a discrete rank* 1 *valuation on* K *compatible with an ordering* β *and let* $(x_n)_{n\in\mathbb{N}}$ *denote a Cauchy sequence of elements of* K*. If* $x_n \not\to 0$*, then there exists* $s \in \{\pm 1\}$ *such that* $x_n \in s\beta$ *for* n *sufficiently large.*

Proof. Let $(x_n)_{n\in\mathbb{N}}$ be a Cauchy sequence such that for all $N \in \mathbb{N}$ there exist $N_1, N_2 \geq N$ such that $x_{N_1} \geq 0$ and $x_{N_2} \leq 0$. It suffices to show that for each $\varepsilon > 0$, there exists an $M \in \mathbb{N}$ such that $|x_r|_\mathfrak{p} \leq \varepsilon$ for all $r \geq M$. Now $(x_n)_{n\in\mathbb{N}}$ being Cauchy, there exists an $N_\varepsilon \in \mathbb{N}$ such that $|x_n - x_m|_\mathfrak{p} < \varepsilon$ for all $n, m \geq N_\varepsilon$. We claim that N_ε is the desired M. Indeed, suppose that there exists $r \geq N_\varepsilon$ such that $|x_r|_\mathfrak{p} > \varepsilon$. Suppose that $x_r > 0$. By assumption, there exists $s \geq N_\varepsilon$ such that $x_s \leq 0$. Hence, $x_r - x_s \geq x_r > 0$. Therefore, $|x_r - x_s|_\mathfrak{p} \geq |x_r|_\mathfrak{p} > \varepsilon$, a contradiction to the choice of N_ε. The case $x_r < 0$ leads to a contradiction in a similar fashion. $\square$

From the above lemma we get an immediate consequence:

COROLLARY 1.30. *Let* $\operatorname{ord}_\mathfrak{p}$ *be a discrete rank* 1 *valuation on* K*. The ordering* β *of* K *is compatible with* $\operatorname{ord}_\mathfrak{p}$ *if and only if* β *can be extended to the field* $K_\mathfrak{p}$*.*

PROPOSITION 1.31 ([31, Proposition 2.9]). *Let* $\beta \in X_K$ *be an ordering and* v *be a valuation compatible with* β*, then* β *induces an ordering* $\overline{\beta}$ *on the residue field* $K(v)$ *such that for every* $u \in U\mathcal{O}_v$*,* $u \in \beta \iff u + \mathfrak{m} \in \overline{\beta}$*.*

The ordering $\overline{\beta}$ in the above proposition is called the *push-down* of β. The following theorem allows us to "count" (often effectively) all the orderings compatible with a given valuation.

BAER–KRULL THEOREM 1.32 ([31, Corollary 3.11]). *Let* $v : K \twoheadrightarrow \Gamma \cup \{\infty\}$ *be a real valuation on* K*. There is a bijection between the set of all the orderings of* K *compatible with* v *and the set* $\operatorname{Hom}(\Gamma/2\Gamma, \mathbb{Z}_2) \times \mathcal{X}_{K(v)}$*.*

If $\operatorname{ord}_\mathfrak{p}$ is a discrete rank 1 valuation, then $\Gamma/2\Gamma = \mathbb{Z}_2$ and so we have the following corollary, which we write down explicitly to simplify further references.

Corollary 1.33. *If* $\operatorname{ord}_{\mathfrak{p}}$ *is a discrete rank* 1 *valuation on* K*, then there are exactly two orderings compatible with* $\operatorname{ord}_{\mathfrak{p}}$ *that push down to a given ordering of the residue field* $K(\mathfrak{p})$*.*

Let us now build a bridge connecting orderings and Witt rings.

Definition 1.34. Let K be a field, a *signature* of K is any ring epimorphism $\sigma : WK \to \mathbb{Z}$.

There is a natural bijection $\sigma \mapsto \ker \sigma$ between the set of signatures of K and the subset of $\operatorname{Spec} WK$ consisting of all the prime ideals $\mathfrak{p}$ of WK satisfying $WK/\mathfrak{p} \cong \mathbb{Z}$ (see e.g. [33, Proposition VIII.7.4]). Let $\sigma : WK \to \mathbb{Z}$ be a signature, then $\beta_\sigma := \{a \in \dot{K} : \sigma\langle a\rangle = 1\} \cup \{0\}$ is an ordering (see [33, Lemma VIII.3.4]). Conversely, if $\beta \in \mathcal{X}_K$ is an ordering, then $\operatorname{sgn}_\beta : WK \to \mathbb{Z}$ defined by

$$\operatorname{sgn}_\beta a := \begin{cases} 1, & \text{if } a \in \beta,\\ -1, & \text{if } a \in -\beta;\end{cases} \qquad \operatorname{sgn}_\beta \langle a_1, \dots, a_n\rangle := \sum_{i=1}^{n} \operatorname{sgn}_\beta a_i$$

is a signature.

Theorem 1.35 ([54, Theorem 19.1.2]). *If* K *is a formally real field, then there is a bijection between the set* $\mathcal{X}_K$ *of orderings and the set of all the signatures of* K*.*

Proposition 1.36 ([54, Theorem 18.3.2]). *If* $\beta \in \mathcal{X}_K$ *is an ordering, then* $\ker \operatorname{sgn}_\beta$ *is generated by classes of* 1*-fold Pfister forms* $\langle\langle -a\rangle\rangle$ *with* $a \in \beta$*.*

Consider now *all* the orderings of a given field K and define a map

$$\operatorname{Sgn} : WK \to \bigoplus_{\beta \in \mathcal{X}_K} \mathbb{Z}, \quad \operatorname{Sgn} \xi := (\operatorname{sgn}_\beta \xi)_{\beta \in \mathcal{X}_K}.$$

This map is called the *total signature* of K. We have the following important result due to A. Pfister concerning the total signature (c.f. [33, Theorem VIII.3.2]). Recall that an element x of a given ring P is *nilpotent* if $x^n = 0$ for some $n \in \mathbb{N}$ and is *torsion* if $nx = 0$ for some $n \in \mathbb{N}$. Denote

$$\operatorname{Tor} P := \bigl\{x \in P : x \text{ is torsion}\bigr\} \quad \text{and} \quad \operatorname{Nil} P := \bigl\{x \in P : x \text{ is nilpotent}\bigr\}.$$

Pfister's Local-Global Principle 1.37. *For a field* K*,* $\ker \operatorname{Sgn} = \operatorname{Tor} WK$*. Moreover, if* $\xi \in \ker \operatorname{Sgn}$*, then* $2^r\xi = 0$ *for some* $r \in \mathbb{N}_0$*.*

Proposition 1.38 ([54, Theorem 19.2.3]). *If* K *is a formally real field, then* $\operatorname{Tor} WK = \operatorname{Nil} WK$*. In particular* $\operatorname{Nil} WK = \ker \operatorname{Sgn}$*.*

It is a well known fact that on a spectrum $\operatorname{Spec} R$ of a ring R one can define the so called *Zariski topology* with a subbasis consisting of sets of the form $\{\mathfrak{p} \in \operatorname{Spec} R : f \notin \mathfrak{p}\}$ with $f \in R$. Consider, thus, the Zariski topology on the prime spectrum of the Witt ring of a formally real filed K. The bijection between $\mathcal{X}_K$

and the subset $\{\mathfrak{p} \in \operatorname{Spec} WK : WK/\mathfrak{p} \cong \mathbb{Z}\} \subset \operatorname{Spec} WK$ induces a topology on the space of orderings $\mathcal{X}_K$ of the field K. The above mentioned subbasis of Zariski topology on $\operatorname{Spec} WK$ translates into a subbasis consisting of the sets

$$H(a) := \bigl\{\beta \in \mathcal{X}_K : a \notin \beta\bigr\}.$$

This topology is called the *Harrison topology* on $\mathcal{X}_K$.

1.3. Knebusch-Milnor exact sequence

This section is fully devoted to the proof of exactness of the Knebusch-Milnor exact sequence (see Theorem 1.40 below) of Witt groups of a Dedekind domain and its field of fractions. This remarkable theorem is the single result most often referenced in this book, hence, unlike the rest of this chapter, we present its (almost complete) proof. This section is mostly based on [39, 55].

Recall (see e.g. [1, 15]) that a *Dedekind domain* is a Noetherian, integrally closed domain of dimension 1. Every localization of a Dedekind domain at a non-zero prime is a discrete valuation ring (see [1, Theorem 9.3]). We will use the following classical result about Dedekind domains:

Proposition 1.39. *If P is a Dedekind domain and M is a finitely generated torsion-free P-module, then M is projective.*

As for the proof of this proposition, we refer the reader to [6, Chapter VII, §4.10, Proposition 22]. Let $K := \operatorname{qf}(P)$ be a field of fractions of a Dedekind domain P. Take $\xi = \langle a_1, \dots, a_n\rangle \in WK$ and fix a non-zero prime $\mathfrak{p} \in \operatorname{Spec} P$. The localization of P at $\mathfrak{p}$ is a valuation ring $\mathcal{O}_\mathfrak{p}$ of K. Choosing a uniformizer $p \in \mathcal{O}_\mathfrak{p}$ we may decompose ξ into

$$\xi = \langle u_1, \dots, u_m\rangle + \langle pu_{m+1}, \dots, pu_n\rangle$$

for some $u_1, \dots, u_n$ invertible in $\mathcal{O}_\mathfrak{p}$. The *second residue homomorphism*[3] is the map $\partial_\mathfrak{p} : WK \twoheadrightarrow WK(\mathfrak{p})$ defined by the formula (c.f. [33, Chapter VI]):

$$\partial_\mathfrak{p}\xi := \langle u_{m+1}(\mathfrak{p}), \dots, u_n(\mathfrak{p})\rangle.$$

Thus, we have two maps: a natural ring morphism $W(P \rightarrowtail K)$ and the group homomorphism $\partial : WK \to \bigoplus WK(\mathfrak{p})$ given by $\partial\xi := \bigl(\partial_\mathfrak{p}\xi\bigr)_\mathfrak{p}$.

Theorem 1.40. *If P is a Dedekind domain and $K := \operatorname{qf}(P)$ its field of fractions, then the following sequence is exact:*

$$0 \to WP \to WK \to \bigoplus_{\substack{\mathfrak{p} \in \operatorname{Spec} P \\ \mathfrak{p} \neq \{0\}}} WK(\mathfrak{p}).$$

[3] The numeral "second" hints that there is also a *first* residue homomorphism. It is indeed true (c.f. [33, Chapter VI]), but we do not have any use for it here.

Chronologically, it was first shown by M. Knebusch that $W(P \rightarrowtail K)$ is a monomorphism and only later J. Milnor proved that the image of WP in WK is actually the kernel of $\partial : WK \to \bigoplus WK(\mathfrak{p})$. Respecting the chronological order, we first prove exactness at WP in Lemma 1.41 and then we prove exactness at WK in Lemma 1.45.

Lemma 1.41. *Under the above assumptions, $W(P \rightarrowtail K)$ is injective.*

Proof. Let (M, ξ) be a f.g. projective module over P together with a non-degenerate bilinear form ξ and suppose that $(M, \xi) \otimes K$ is hyperbolic. We must show that (M, ξ) itself is hyperbolic (more generally metabolic, but remember our general assumption that $1/2 \in UP$). The module $V := M \otimes K$ is a vector space over K spanned by $M \otimes \{1\}$. Identifying $m \in M$ with $m \otimes 1 \in V$, we may treat M as a generating subset of V. We will again use the symbol ξ for the associated bilinear form on V.

Since (V, ξ) is hyperbolic, thus it contains a self-orthogonal subspace $W = W^{\perp} < V$. Take $N := M \cap W$ a submodule of M. We claim that $N = N^{\perp}$. Indeed, let $x \in N$. For every $y \in N$, elements x, y are orthogonal since both belong to self-orthogonal subspace W. It follows that $x \in N^{\perp}$ and so $N \subseteq N^{\perp}$. Conversely, let $x \in N^{\perp}$ and take any $w \in W$. The element w can be expressed as a linear combination of elements from N with coefficients in $K = \mathrm{qf}(P)$. If d is the common denominator of these coefficients, then dw lies in N. Now x and dw are orthogonal hence $x \in W^{\perp} = W$. It follows that $x \in N = W \cap M$. This proves our claim.

The quotient module M/N is a subset of the vector space V/W. As such it is clearly torsion-free. It is also finitely generated since M is. Proposition 1.39 assert that N is projective. Consequently the exact sequence $N \rightarrowtail M \twoheadrightarrow M/N$ splits. Therefore $N = N^{\perp}$ is a direct summand of M. It follows that (M, ξ) is hyperbolic. $\square$

Before we prove the exactness of the Knebusch-Milnor sequence at WK we need to introduce a notion of a *lattice* (c.f. [39, §IV.3]).

Definition 1.42. Let V be a finitely dimensional K-vector space with some basis $\mathscr{B} = \{v_1, \dots, v_n\}$. A *$P$-lattice* in V is a P-module $L = Pv_1 + \cdots + Pv_n$.

It follows from Proposition 1.39 that a P-lattice is a projective module. In the proof of Milnor's part we will make use of the following lemma (we omit the proof, referring the reader to [41]).

Lemma 1.43 ([41, 81:14]). *Let V be a vector space over K and for each $\mathfrak{p} \in \operatorname{Spec} P$ let $J_{\mathfrak{p}}$ be an $\mathcal{O}_{\mathfrak{p}}$-lattice in V. If there is a P-lattice L_1 such that $L_1 \otimes \mathcal{O}_{\mathfrak{p}} = J_{\mathfrak{p}}$ for almost all $\mathfrak{p}$, then there is a P-lattice L such that $L \otimes \mathcal{O}_{\mathfrak{p}} = J_{\mathfrak{p}}$ for every $\mathfrak{p} \in \operatorname{Spec} P$.*

Lemma 1.44. *Let $\operatorname{ord}_{\mathfrak{p}}$ be the discrete rank-1 valuation on K associated with a valuation ring $(\mathcal{O}_{\mathfrak{p}}, \mathfrak{p})$, then $\operatorname{im} W(\mathcal{O}_{\mathfrak{p}} \rightarrowtail K) = \ker \partial_{\mathfrak{p}}$.*

Proof. Since a valuation ring (associated with a discrete rank-1 valuation) is a Dedekind domain, it follows from Lemma 1.41 that $W(\mathcal{O}_\mathfrak{p} \rightarrowtail K)$ is injective, hence we may identify $W\mathcal{O}_\mathfrak{p}$ with a its image $\operatorname{im} W(\mathcal{O}_\mathfrak{p} \rightarrowtail K)$ in the Witt ring WK. The ring $\mathcal{O}_\mathfrak{p}$ is local, therefore by Proposition 1.7 any bilinear form ξ over $\mathcal{O}_\mathfrak{p}$ has a diagonalization $\xi = \langle u_1, \dots, u_n\rangle$ with $u_1, \dots, u_n$ invertible in $\mathcal{O}_\mathfrak{p}$. It is obvious that $\partial_\mathfrak{p}\xi = 0$.

Conversely assume that $\xi \in \ker \partial_\mathfrak{p} \subset WK$. Since we are working over a field here, we may assume that ξ is anisotropic and has a diagonalization $\langle u_1, \dots, u_m\rangle \perp \langle pu_{m+1}, \dots, pu_n\rangle$ with p being a fixed uniformaizer (we used it already to define $\partial_\mathfrak{p}$) and some units $u_1, \dots, u_n \in U\mathcal{O}_\mathfrak{p}$. Since $\xi \in \ker \partial_\mathfrak{p}$, thus the form $\langle u_{m+1}(\mathfrak{p}), \dots, u_n(\mathfrak{p})\rangle$ over the residue field $K(\mathfrak{p}) = \mathcal{O}_\mathfrak{p}/\mathfrak{p}$ is hyperbolic. It follows that $n - m$ is even and $\partial_\mathfrak{p}\xi$ has a matrix $\left(\begin{smallmatrix} 0 & I \\ I & 0 \end{smallmatrix}\right)$ in some basis $\overline{\alpha_{m+1}}, \dots, \overline{\alpha_n}$. Take now $\alpha_{m+1}, \dots, \alpha_n \in V$ such that $\alpha_i(\mathfrak{p}) = \overline{\alpha_i}$ and let L_1 be the $\mathcal{O}_\mathfrak{p}$-lattice spanned by $\alpha_{m+1}, \dots, \alpha_n$. It follows that in this basis the bilinear form $\langle u_{m+1}, \dots u_n\rangle$ has a matrix $\left(\begin{smallmatrix} M_1 & M_2+I \\ M_2+I & M_3 \end{smallmatrix}\right)$ where M_1, M_2 M_3 have all their coefficients in $\mathfrak{p}$. Now let L be the following $\mathcal{O}_\mathfrak{p}$-lattice

$$L = \mathcal{O}_\mathfrak{p}\alpha_{m+1} + \dots + \mathcal{O}_\mathfrak{p}\alpha_{m+(n-m)/2} + \mathcal{O}_\mathfrak{p}\bigl(\tfrac{1}{p}\alpha_{m+1+(n-m)/2}\bigr) + \dots + \mathcal{O}_\mathfrak{p}\bigl(\tfrac{1}{p}\alpha_n\bigr).$$

Then with respect to the basis spanning L, the form $\langle pu_{m+1}, \dots, pu_n\rangle$ has a matrix $A = \left(\begin{smallmatrix} pM_1 & M_2+I \\ M_2+I & {}^1\!/_p M_3 \end{smallmatrix}\right)$ with entries in $\mathcal{O}_\mathfrak{p}$. Now $(\det A)(\mathfrak{p}) = \det\left(\begin{smallmatrix} * & I \\ I & 0 \end{smallmatrix}\right) = (-1)^{(n-m)/2}$. Hence A is invertible over $\mathcal{O}_\mathfrak{p}$. It follows that $\langle pu_{m+1}, \dots, pu_n\rangle$ and so also ξ are non-degenerate forms over $\mathcal{O}_\mathfrak{p}$. □

We are now ready to show that the Knebusch-Milnor sequence is exact also at the Witt group of K.

LEMMA 1.45. *If P is a Dedekind domain and K is its field of fractions, then* $\operatorname{im} W(P \rightarrowtail K) = \ker \partial$.

Proof. As before, we treat WP as a subring of WK by virtue of Lemma 1.41. For every $\mathfrak{p} \in \operatorname{Spec} P$ the map $W(P \rightarrowtail \mathcal{O}_\mathfrak{p})$ is injective, hence by the previous lemma

$$WP \subseteq \bigcap_{\substack{\mathfrak{p}\in\operatorname{Spec} P\\ p\neq\{0\}}} W\mathcal{O}_\mathfrak{p} = \bigcap_{\substack{\mathfrak{p}\in\operatorname{Spec} P\\ \mathfrak{p}\neq\{0\}}} \ker \partial_\mathfrak{p},$$

consequently $WP \subseteq \ker \partial$.

Conversely, let $\xi : V \times V \to K$ be a bilinear form over K such that $\partial\xi$ vanishes in $\bigoplus WK(\mathfrak{p})$. Fix a basis $\mathscr{B} = \{v_1, \dots, v_n\}$ of V and let $S_1 \subset \operatorname{Spec} P$ be the set of all the poles of $\xi(v_i, v_j)$ for $1 \le i, j \le n$, that is:

$$S_1 := \Bigl\{\mathfrak{p} \in \operatorname{Spec} P : \exists_{1\le i,j\le n} \operatorname{ord}_\mathfrak{p} \xi(v_i, v_j) < 0\Bigr\}.$$

Next, let $S_2 \subset \operatorname{Spec} P$ be the set of all the zeros and poles of $\det \xi$:

$$S_2 := \bigl\{\mathfrak{p} \in \operatorname{Spec} P : \operatorname{ord}_\mathfrak{p} \det \xi \neq 0\bigr\}.$$

Finally, let $S := S_1 \cup S_2$. Clearly S is a finite set and for every non-zero prime ideal $\mathfrak{p} \in \operatorname{Spec} P \setminus S$ the form $\xi \big|_{L_\mathfrak{p} \times L_\mathfrak{p}}$ on a $\mathcal{O}_\mathfrak{p}$-lattice $L_\mathfrak{p} = \mathcal{O}_\mathfrak{p} v_1 + \cdots + \mathcal{O}_\mathfrak{p} v_n$ is non-degenerate. Using Lemma 1.44, for each $\mathfrak{p} \in S$ find a $\mathcal{O}_\mathfrak{p}$-lattice $L_\mathfrak{p}$ such that $\xi \big|_{L_\mathfrak{p} \times L_\mathfrak{p}}$ is non-degenerate, either. Now, Lemma 1.43 asserts that there is a P-lattice L such that $\xi \big|_{L \times L}$ is non-degenerate. It follows that $\xi \in WP$. $\square$

For a Dedekind domain P and its field of fractions $K = \operatorname{qf}(P)$ we denote

$$\mathbb{E}(P) := \big\{a \in \dot K/\dot K^2 : \operatorname{ord}_\mathfrak{p} a \equiv 0 \pmod 2 \text{ for every } \mathfrak{p} \in \operatorname{Spec} P, \mathfrak{p} \neq \{0\}\big\}.$$

If it is clear from the context what ring we mean, we will tend to simplify the notation and write $\mathbb{E}$ instead of $\mathbb{E}(P)$. We have the following consequences of exactness of the Knebusch-Milnor sequence.

Corollary 1.46. *Let $a \in \dot K/\dot K^2$ be a square class, then $a \in \mathbb{E}$ if and only if the unary form $\langle a\rangle$ belongs to WP, i.e.*

$$a \in \mathbb{E} \iff \langle a\rangle \in WP.$$

Proof. A unary form $\langle a\rangle$ lies in WP if and only if it is in the kernel of ∂ if and only if a is the local unit for every $\mathfrak{p} \in \operatorname{Spec} P$ if and only if the square class of a lies in $\mathbb{E}$. $\square$

Corollary 1.47. *Let ξ be a form over K, then $\xi \in WP$ implies that* $\operatorname{disc} \xi \in \mathbb{E}$.

Proof. For a point $\mathfrak{p} \in \operatorname{Spec} P$ we can write $\xi = \xi' + p\xi''$ where p is a uniformizer of $\mathfrak{p}$ and ξ', ξ'' are some forms over the local field $K_\mathfrak{p}$. Computing the second residue homomorphism, we have $0 = \partial_\mathfrak{p}(\xi) = \overline{\xi''}$ by Theorem 1.40. Hence the dimension of ξ'' is even, consequently $\operatorname{ord}_\mathfrak{p}(\operatorname{disc} \xi) \equiv 0 \pmod 2$. $\square$

It is obvious that if P is a subring of a ring R, then $\operatorname{Nil} P = P \cap \operatorname{Nil} R$. Hence, we have one more consequence of Knebusch-Milnor theorem, which we will need much later.

Observation 1.48. *If P is a Dedekind domain and $K = \operatorname{qf}(P)$, then* $\operatorname{Nil} WP = WP \cap \operatorname{Nil} WK$.

1.4. Introduction to real curves

This section is aimed to be a brief introduction into some aspects of the theory of real algebraic curves. We present here only a very limited part of this theory, restricting ourselves only to the results utilized later. As in the rest of this chapter, we omit all the proofs, instead giving only the bibliographical references. We wholeheartedly, however, encourage the reader interested in the subject to refer to the standard positions in the field like [5, 21, 22].

Throughout this section, $\Bbbk$ will always denote a fixed real closed field. Consider an algebraic function field (of one variable) K with the field of constants $\Bbbk$. Take $\Omega := \Omega(K)$ to be the set of all the proper valuation rings of K containing $\Bbbk$:

$$\Omega(K) := \big\{(\mathcal{O}_\mathfrak{p}, \mathfrak{p}) : \Bbbk \subsetneq \mathcal{O}_\mathfrak{p} \subsetneq K,\ \mathcal{O}_\mathfrak{p} \text{ a valuation ring}\big\}.$$

Since each valuation ring is uniquely determined by its maximal ideal, we tend to simplify notation and write $\mathfrak{p}$ alone, instead of $(\mathcal{O}_\mathfrak{p}, \mathfrak{p})$. All these maximal ideals are in fact closed points of the scheme associated with K. We will shortly call them *points* (or sometimes *primes*) of K. This should not lead to any confusion, since we never make any reference to the generic point of this scheme.

The residue field $K(\mathfrak{p}) = \mathcal{O}_\mathfrak{p}/\mathfrak{p}$ of a given point $\mathfrak{p}$ is a finite extension of the (real closed) field $\Bbbk$. Hence, it is either $\Bbbk$ itself if $\mathcal{O}_\mathfrak{p}$ is residually real, or the algebraic closure $\Bbbk(\sqrt{-1})$, when $\mathcal{O}_\mathfrak{p}$ is not residually real. The set of real points will be denoted by γ_K (or just γ if the field is clear from the context). The set Ω can be treated as a projective algebraic curve over $\Bbbk$. Indeed, using [51, Proposition III.9.2] write $K = \Bbbk(x, y)$ for some $x, y \in K$ and let $F \in \Bbbk[X, Y]$ be an irreducible polynomial satisfying $F(x, y) = 0$. Then Ω is isomorphic to the projective closure of $\{F = 0\}$. Consequently γ is a *real algebraic curve* and may be embedded into the projective plane $\mathbb{P}^2\Bbbk$ (or even into the affine space $\mathbb{A}^9\Bbbk$, since $\mathbb{P}^2\Bbbk$ injects into $\mathbb{A}^9\Bbbk$ by [5, Theorem 3.4.4]). We treat elements of K as functions on γ in the usual fashion.

The real closed field $\Bbbk$ admits a natural topology defined by its unique ordering. The subbasis of this topology consists of open intervals $(a, b) := \{x \in \Bbbk : a < x < b\}$. This topology extends canonically to $\mathbb{A}^2\Bbbk$ and further to $\mathbb{P}^2\Bbbk$. The embedding $\gamma \rightarrowtail \mathbb{P}^2\Bbbk$ defines a topology on γ. We shall refer to it as the *Euclidean topology*[4] on γ. This is the coarsest topology such that every $f \in K$ is continuous as a function on γ (see e.g. [21]).

The field $\Bbbk$, being real closed, has the unique ordering: $x < y \iff y - x \in \Bbbk^2$. By Baer-Krull theorem (see Corollary 1.33), there are exactly two orderings β_1, β_2 for K compatible with a given real point $\mathfrak{p}$. The best explicit characterization of these two orderings utilizes the notion of curve intervals, hence we have to postpone it till page 26. An alternative description is the following one: let $\mathfrak{p}$ be a point on γ. Fix an affine plane containing $\mathfrak{p}$. Let $B(\mathfrak{p}, r)$ denote the open disc centered at $\mathfrak{p}$ and with radius $r \in \Bbbk$. If r is small enough the intersection of γ with $B(\mathfrak{p}, r)$ is homeomorphic to a interval in $\Bbbk$. Take now any non-zero function $f \in K$. Decreasing possibly the radius r even further we may ensure that f has no zeros on the arc $C = \gamma \cap B(\mathfrak{p}, r)$ except possibly in $\mathfrak{p}$. Once we exclude $\mathfrak{p}$ from it, the arc C decomposes into a disjoint sum of two sub-arcs C_1 and C_2, with f having no zeros on any of them. Assume that the two arcs are indexed coherently for all possible functions $f \in K$. We say that f is positive with respect to β_i if $f(\mathfrak{q}) \in \Bbbk^2$

[4] In [21, 22] this is called a *strong topology*, instead.

for all $\mathfrak{q} \in C_i$. Define the *sign at a point* $\mathfrak{p}$ of a non-zero element $f \in K$ by the formula

$$\operatorname{sgn}_{\mathfrak{p}} f := \begin{cases} 1, & \text{if } f \in \beta_1 \cap \beta_2 \\ 0, & \text{if } f \in (\beta_1 \setminus \beta_2) \cup (\beta_2 \setminus \beta_1) \\ -1, & \text{if } -f \in \beta_1 \cap \beta_2. \end{cases}$$

The sign of any square is 1 at every point $\mathfrak{p}$ of γ and so $\operatorname{sgn}_{\mathfrak{p}}$ is well defined on square classes of K.

OBSERVATION 1.49 ([21, §2]). $\operatorname{sgn}_{\mathfrak{p}} f = 0 \iff \operatorname{ord}_{\mathfrak{p}} f \equiv 1 \pmod 2$.

We say that f is *definite* at $\mathfrak{p}$ if $\operatorname{ord}_{\mathfrak{p}} f \equiv 0 \pmod 2$. The notion of a sign at a point extends naturally to quadratic forms. If $\xi = \langle f_1, \ldots, f_n \rangle$ is a quadratic form over K, then

$$\operatorname{sgn}_{\mathfrak{p}} \xi := \sum_{i=1}^{n} \operatorname{sgn}_{\mathfrak{p}} f_i.$$

A form is *definite* if $|\operatorname{sgn}_{\mathfrak{p}} \xi| = \dim \xi$.

Remark 1.50. Do not confuse the "sign at a point" introduced above with the "signature" in the sense of Definition 1.34. In general, the sign at a point does not preserve multiplication (hence is not a ring homomorphism). Take for example $K = \mathbb{R}(X)$ and let $\mathfrak{p}$ be the point $X \cdot \mathbb{R}(X)$ (i.e. $\mathfrak{p}$ is associated with $(0:1) \in \mathbb{P}^1\mathbb{R}$). Then $\operatorname{sgn}_{\mathfrak{p}}\langle x \rangle = 0$ but $\operatorname{sgn}_{\mathfrak{p}}(\langle x \rangle \otimes \langle x \rangle) = 1$.

Introduce a relation $\sim$ on γ saying that two points $\mathfrak{p}$, $\mathfrak{q}$ are in the relation $\mathfrak{p} \sim \mathfrak{q}$ if and only if $\operatorname{sgn}_{\mathfrak{p}} f = \operatorname{sgn}_{\mathfrak{q}} f$ for every f definite on the whole γ. The equivalence classes of this relation are called *components* of γ (see [21]). These are precisely the *semi-algebraically connected components* in the sense of [5]. For the proof that the two notions coincide one may use [21, Proposition 2.9] and [14, Proposition 11.1] or equivalently [5, Corollary 15.1.8 and Theorem 15.2.3]—see also the discussion at the end of [5, Chapter 15].

PROPOSITION 1.51. *A real algebraic curve γ consists of finitely many semi-algebraically connected components. Each component is homeomorphic to a unit circle.*

For the proof see [21, Corollary 2.8] and the discussion following it. Denote the components by $\gamma_1, \ldots, \gamma_N$. Any such component can be singled out by the sign of an element of K as the following theorem shows.

THEOREM 1.52 ([21, Theorem 2.10]). *Let $\gamma_1, \ldots, \gamma_N$ be the components of γ and let $\varepsilon_1, \ldots, \varepsilon_N \in \{\pm 1\}$ be prescribed signs. Then there exists a function $f \in K$ definite on γ and such that the function $\mathfrak{p} \mapsto \operatorname{sgn}_{\mathfrak{p}} f$ is constant and equal ε_i on each γ_i.*

Recall that a function $f \in K$ has an odd order at a point $\mathfrak{p}$ if and only if f is positive with respect to one ordering compatible with $\mathfrak{p}$ and negative with respect to the other one. If this is the case, we say that f *changes sign* at $\mathfrak{p}$. As a geometrical intuition suggest, on a single component a function may change sign only at even number of points.

THEOREM 1.53 ([21, Theorem 3.4]). *For every $f \in K$ and every component γ_i of γ, the number of points $\mathfrak{p} \in \gamma_i$ at which f changes sign is finite and even.*

THEOREM 1.54 ([21, Theorem 4.5]). *Given an even number of points in each component γ_i of γ, there exists a function $f \in K$ which changes sign precisely at these points.*

Suppose that the curve γ consists of N components $\gamma_1, \dots, \gamma_N$. Each component is homeomorphic to a circle, hence one can choose two possible orientations of each component. This sums up to a total 2^N orientations of γ (see [21, §5]). From now on, we assume that one such an orientation is arbitrary chosen and fixed. This permits us to define intervals on γ (c.f. [21, §6]). Let $\mathfrak{p}$, $\mathfrak{q}$ be two distinct points belonging to the same component γ_i of γ. An *open interval* $(\mathfrak{p}, \mathfrak{q})$ consists of precisely these points $\mathfrak{r} \in \gamma_i$ such that $\mathfrak{r}$ is in-between $\mathfrak{p}$ and $\mathfrak{r}$ with respect to the fixed orientation of γ. The component γ_i is then the disjoint sum of the sets $(\mathfrak{p}, \mathfrak{q})$, $(\mathfrak{q}, \mathfrak{p})$, $\{\mathfrak{p}\}$ and $\{\mathfrak{q}\}$ (see [21, Proposition 6.4]). A *closed interval* $[\mathfrak{p}, \mathfrak{q}]$ is by definition $[\mathfrak{p}, \mathfrak{q}] := \gamma_i \setminus (\mathfrak{q}, \mathfrak{p}) = \{\mathfrak{p}\} \cup (\mathfrak{p}, \mathfrak{q}) \cup \{\mathfrak{q}\}$. It follows from Theorems 1.52 and 1.54 above, that for every interval $(\mathfrak{p}, \mathfrak{q}) \subset \gamma_i$ there is a function $\chi_{(\mathfrak{p},\mathfrak{q})} \in K$ such that

$$\operatorname{sgn}_{\mathfrak{r}} \chi_{(\mathfrak{p},\mathfrak{q})} = \begin{cases} 1, & \text{if } \mathfrak{r} \in \gamma \setminus \gamma_i \text{ or } \mathfrak{r} \in (\mathfrak{q}, \mathfrak{p}), \\ 0, & \text{if } \mathfrak{r} \in \{\mathfrak{p}, \mathfrak{q}\}, \\ -1, & \text{if } \mathfrak{r} \in (\mathfrak{p}, \mathfrak{q}). \end{cases}$$

The function $\chi_{(\mathfrak{p},\mathfrak{q})}$ is unique, up to a multiplication by a sum of squares, and is called an *interval function* of $(\mathfrak{p}, \mathfrak{q})$.

The notion of orientation of γ makes it possible to explicitly describe the two orderings β_+ and β_- compatible with a given real point $\mathfrak{p} \in \gamma_i$. Namely

$$\beta_+ = \Big\{ f \in K : \exists_{\mathfrak{q}\in\gamma_i} \forall_{\mathfrak{r}\in(\mathfrak{p},\mathfrak{q})} f(\mathfrak{r}) > 0 \Big\}, \quad \beta_- = \Big\{ f \in K : \exists_{\mathfrak{q}\in\gamma_i} \forall_{\mathfrak{r}\in(\mathfrak{q},\mathfrak{p})} f(\mathfrak{r}) > 0 \Big\}.$$

In the last two chapters, we make extensive use of the following result originally due to E. Witt in case $\Bbbk = \mathbb{R}$ and generalized to the general case by R. Elman, T.Y. Lam, A. Prestel (see [16, p. 298]) and M. Knebusch (see [22, Theorem 9.4]).

WITT THEOREM 1.55. *If ξ is a quadratic form over K, $\dim \xi \geq 3$ and ξ is indefinite (i.e. $|\operatorname{sgn}_{\mathfrak{p}} \xi| \leq \dim \xi$) for almost all $\mathfrak{p} \in \gamma$, then ξ is isotropic.*

The above theorem may be consider as a version of a Strong Hasse Principle. The corresponding Weak Hasse Principle follows immediately:

COROLLARY 1.56 ([22, Theorem 9.5]). *If ξ, ζ are two forms over K with $\dim \xi = \dim \zeta$, $\operatorname{disc} \xi = \operatorname{disc} \zeta$ and $\operatorname{sgn}_{\mathfrak{p}} \xi = \operatorname{sgn}_{\mathfrak{p}} \zeta$ for almost all $\mathfrak{p} \in \gamma$, then $\xi \cong \zeta$.*

Consider now a subring R of K consisting of all functions having no poles on γ:

$$R := \bigcap_{\mathfrak{p}\in\gamma} \mathcal{O}_{\mathfrak{p}}.$$

We call it the *ring of regular functions* on the real curve γ. It is a Dedekind domain by [51, Proposition III.2.5]. Hence we consider the Knebusch-Milnor exact sequence associated with R (c.f. Theorem 1.40). In this particular case, however, we know more. In fact we can cap the sequence from the right. Observe that for any real point $\mathfrak{p}$ of K, we have $K(\mathfrak{p}) = \Bbbk$, hence $WK(\mathfrak{p}) \cong \mathbb{Z}$. Therefore, there is a natural isomorphism $\bigoplus_{\mathfrak{p}\in\gamma} WK(\mathfrak{p}) \cong \mathbb{Z}^{(\gamma)}$, where $\mathbb{Z}^{(\gamma)}$ denotes a coproduct of $\operatorname{card}(\gamma)$ copies of $\mathbb{Z}$. In what follows we identify these two groups. We have natural mappings between WK, $\bigoplus_{\mathfrak{p}\in\gamma} WK(\mathfrak{p})$ and $\mathbb{Z}^N$. Namely, the second residue homomorphism $\partial : WK \to \bigoplus_{\mathfrak{p}\in\gamma} WK(\mathfrak{p})$ defined by the condition that $\mathfrak{p}$-th coordinate of $\partial(\langle f_1, \dots, f_n, pf_{n+1}, \dots, pf_m\rangle) = \operatorname{sgn} f_{n+1}(\mathfrak{p}) + \dots + \operatorname{sgn} f_m(\mathfrak{p})$, where p is a fixed uniformizer of $\mathfrak{p}$ and all f_i are units. Secondly $\lambda : \bigoplus_{\mathfrak{p}\in\gamma} WK(\mathfrak{p}) \cong \mathbb{Z}^{(\gamma)} \to \mathbb{Z}^N$ assigns to the sequence $(n_{\mathfrak{p}})_{\mathfrak{p}\in\gamma} \in \mathbb{Z}^{(\gamma)}$ the N-tuple $(n_1, \dots, n_N)$ where $n_i = \sum_{\mathfrak{p}\in\gamma_i} n_{\mathfrak{p}}$.

Theorem 1.57 ([22, Theorem 11.2]). *The following sequence is exact*

$$0 \to WR \xrightarrow{i} WK \xrightarrow{\partial} \bigoplus_{\mathfrak{p}\in\gamma} WK(\mathfrak{p}) \xrightarrow{\lambda} \mathbb{Z}^N \to 0.$$

One may notice that in [22] the above sequence is written for the Witt ring $W\Omega$ and so has a slightly different form, but the adaptation to our situation is immediate. In Chapter 4 we show that this sequence actually splits.

2

Local quadratic extensions

In this chapter we deal with the Witt functor of the natural injection $P \rightarrowtail P[\sqrt{d}]$, where P is a local ring (and d is not a square, of course). Hence, in this whole chapter we use the following notation:

- P is a local domain in which 2 is invertible,
- $\mathfrak{m}$ is the maximal ideal of P,
- $d \in P$ is a fixed non-square,
- $P \rightarrowtail P[\sqrt{d}]$ denotes the canonical injection.

If d is invertible in P then the ring extension $P \subset P[\sqrt{d}]$ is called *unitary*, otherwise it is called *non-unitary*. In the first case it is clear that $\langle 1, -d\rangle$ is hyperbolic over $P[\sqrt{d}]$ but not over P. Consequently, its Witt class belongs to the kernel of $W(P \rightarrowtail P[\sqrt{d}])$ which, thus, cannot be a monomorphism. If, in addition, $P[\sqrt{d}]$ is free as a P-module more can be said.

Proposition 2.1 ([2, Corollary 4.11]). *If P is a semi-local ring, $d \in UP$ and $P \subsetneq P[\sqrt{d}]$ is a unitary quadratic extension such that $P[\sqrt{d}]$ is a free P-module, then* $\ker W(P \rightarrowtail P[\sqrt{d}]) = \langle\langle -d\rangle\rangle \cdot WP$.

Now, we turn our attention to non-unitary extensions. Therefore, from now on, d is a fixed noninvertible element of P. We shall describe the structure of $P[\sqrt{d}]$. First, however, we need the following general lemma. It can easily be considered "well known", unfortunately, in most sources it is proved only for Noetherian local rings (see e.g. [6, Chapter IV, §2.5, Corollary 3]), but it is true also without the Noetherian assumption.

Lemma 2.2. *Let $(P, \mathfrak{m})$ be a local ring and assume that P is a subring of a ring R with R being finitely generated as a P-module. Then R is semi-local.*

Proof. Denote the residue field $P/\mathfrak{m}$ by k. It is clear that $\mathfrak{m}R$ is contained in every maximal ideal of R. Take k' to be the quotient ring $R/\mathfrak{m}R$. It is a P-module and since $\mathfrak{m}$ is mapped to zero in the composition $P \rightarrowtail R \twoheadrightarrow R/\mathfrak{m}R$, hence k' is a k-vector space (actually a k-algebra). By the assumption, R is a finitely generated P-module, consequently k' is finitely dimensional as a k-vector space. It follows from [1, Proposition 6.10] that k' is an Artinian ring, hence it is semi-local by [15, Theorem 2.14]. Consequently, R itself is semi-local. $\square$

THEOREM 2.3. *With the above notation, $P[\sqrt{d}]$ is a local ring, $\mathfrak{m} + P \cdot \sqrt{d}$ is its maximal ideal and $UP + P \cdot \sqrt{d}$ is the group of units of $P[\sqrt{d}]$.*

Proof. It is clear that $\mathfrak{m} + P \cdot \sqrt{d}$ is an ideal of $P[\sqrt{d}]$. Thus, if we prove that $UP + P \cdot \sqrt{d} = P[\sqrt{d}] \setminus (\mathfrak{m} + P \cdot \sqrt{d})$ is the group of units of $P[\sqrt{d}]$, it will follow that $P[\sqrt{d}]$ is a local ring. The ring $P[\sqrt{d}]$ is semi-local by Lemma 2.2 and let $M_1, \dots, M_n$ be its maximal ideals. Then $\mathfrak{m} = M_i \cap P$ for every $1 \le i \le n$. Now, since d lies in $\mathfrak{m}$, thus $\sqrt{d}$ must belong to all the maximal ideals M_i and so $\sqrt{d}$ is an element of the Jacobson's radical $\operatorname{Rad}(P[\sqrt{d}])$ of $P[\sqrt{d}]$.

Take now an invertible element $a + b\sqrt{d} \in UP[\sqrt{d}]$. There exists $x + y\sqrt{d}$ such that

$$1 = \big(a + b\sqrt{d}\big)\big(x + y\sqrt{d}\big) = ax + byd + (ay + bx)\sqrt{d}.$$

Now both the elements d and $\sqrt{d}$ are in the Jacobson's radical of $P[\sqrt{d}]$. Therefore ax must be invertible in $P[\sqrt{d}]$, since otherwise the whole right hand side of the above equation would belong to some maximal ideal M_i, which is clearly impossible. It follows that $a \in UP[\sqrt{d}] \cap P$ and so a is invertible in P. This shows one inclusion, namely $UP[\sqrt{d}] \subseteq UP + P \cdot \sqrt{d}$.

Conversely, take an element $a + b\sqrt{d}$ with a invertible in P. We know that P is a local ring and d belongs to its maximal ideal $\mathfrak{m}$, thus $a^2 - b^2 d$ must also be invertible. Now the element $a^2 - b^2 d$ is the determinant of the following system of linear equations over P:

$$\begin{cases} ax + byd = 1 \\ bx + ay = 0. \end{cases}$$

Consequently, this system has a solution $x, y \in P$; rewriting it over $P[\sqrt{d}]$ we have $(a + b\sqrt{d})(x + y\sqrt{d}) = 1$ and so $a + b\sqrt{d}$ is invertible in $P[\sqrt{d}]$. $\square$

Now, as $(P, \mathfrak{m})$ and $(P[\sqrt{d}], \mathfrak{m} + P \cdot \sqrt{d})$ are both local, we may consider their residue fields. It is clear that $x + y\sqrt{d}$ is mapped by the canonical epimorphism to the same element as x itself. Hence we arrive at the following:

OBSERVATION 2.4. *The residue fields $P/\mathfrak{m}$ and $P[\sqrt{d}]/(\mathfrak{m} + P \cdot \sqrt{d})$ are isomorphic.*

Craven, Rosenberg and Ware proved the following result:

THEOREM 2.5 ([13, Proposition 2.1]). *If $(P, \mathfrak{m})$ is a regular Noetherian local ring and K is its field of fractions, then*

$$\ker W(P \rightarrowtail K) \subset \ker W(P \twoheadrightarrow P/\mathfrak{m}).$$

An immediate consequence of the previous observation is the following analogy of this theorem:

COROLLARY 2.6. *Under the above assumptions,*

$$\ker W\big(P \rightarrowtail P[\sqrt{d}]\big) \subset \ker W(P \twoheadrightarrow P/\mathfrak{m}).$$

Moreover, if $P[\sqrt{d}]$ *is regular, then* $\ker W(P \rightarrowtail K) \subset \ker W(P \twoheadrightarrow P/\mathfrak{m})$*, where* $K := \operatorname{qf}(P[\sqrt{d}])$ *denotes the field of fractions of* $P[\sqrt{d}]$*.*

Proof. By Observation 2.4, the following diagram commutes

$$\begin{tikzcd} P \arrow[rr, tail] \arrow[dr, two heads] & & P[\sqrt{d}] \arrow[dl, two heads] \\ & P/\mathfrak{m} & \end{tikzcd}$$

Applying the Witt functor to it, we get another commutative diagram

$$\begin{tikzcd} WP \arrow[rr, tail] \arrow[dr, two heads] & & WP[\sqrt{d}] \arrow[dl, two heads] \\ & WP/\mathfrak{m} & \end{tikzcd}$$

Consequently, every element which is already killed by the horizontal arrow must be mapped to the class of hyperbolic forms in $W(P \rightarrowtail P/\mathfrak{m})$, as well. The moreover part follows immediately from Theorem 2.5. $\square$

We show one more consequence of Theorem 2.3. It will be needed much later in this chapter, but here is a convenient place to state it, as it does not use the transfer technique discussed in the next section.

PROPOSITION 2.7. *The group* UP *of units of* P *is quadratically closed under the ring extension* $P \subset P[\sqrt{d}]$ *in the sense that*

$$\big(P[\sqrt{d}]\big)^2 \cap UP = P^2 \cap UP.$$

In other words, the proposition asserts that every unit $u \in UP$ which is a square in $P[\sqrt{d}]$ is already a square in P.

Proof. Take a unit $u \in UP$ and suppose that it is a square in $P[\sqrt{d}]$, so $u = (a+b\sqrt{d})^2$. Consequently $a+b\sqrt{d}$ is invertible in $P[\sqrt{d}]$. By Theorem 2.3 it means that a is invertible in P. Expanding the square and rearranging terms we have

$$2ab\sqrt{d} = u - a^2 - b^2 d \in R.$$

But since both 2 and a are invertible, we see that already $b\sqrt{d} \in P$. Consequently $a + b\sqrt{d} \in P$ therefore u is a square in P. $\square$

2.1. Transfer maps

Scharlau's transfer is a very powerful and hard to overestimate tool used to analyze the Witt functor of field extensions (see e.g. [33, Chapter VII, § 1]). Briefly speaking, if $K \subset L$ are two fields ($\operatorname{char} K \neq 2$) and $s : L \to K$ is a K-linear map, then for any quadratic form q over L we define the quadratic form $s_* q$ over K by taking a composition $s \circ q$. The map s_* turns out to preserve orthogonal sums and sends hyperbolic forms to hyperbolic forms, hence it induces a *group* homomorphism of Witt groups $WL \to WK$, which we again denote by s_*.

It is tempting to repeat this procedure for a ring extension $P \subset Q$ and it does indeed work providing that Q is a free module over the base ring (c.f. [36, Section 5.4]). Unfortunately, in the situation we wish to consider (i.e. a ring normalization), this assumption is simply not satisfied. There are two (interconnected) obstacles that we meet. Firstly, if a bigger ring Q is not a free module over the base ring P, then a projective/free module M over Q will not in general be projective over P. Therefore any information we may obtain from a transfer map will not apply to Witt rings. Secondly, if $P \subset P[\sqrt{d}]$ is a quadratic extension[1], then every P-linear functional $P[\sqrt{d}] \to P$ has a form $x + y\sqrt{d} \mapsto x\alpha + y\beta$ for some $\alpha, \beta \in P$. However if $P[\sqrt{d}]$ is not free over P, not every two scalars α, β give rise to a well defined map. The relations between generators 1, $\sqrt{d}$ of the P-module $P[\sqrt{d}]$, which prevent it from being a free P-module, do interfere here, too. Unfortunately, in what follows, we need to consider pairs that do not induce any well defined P-linear map $P[\sqrt{d}] \to P$ (see e.g. Theorem 2.17).

We are going to extend the definition of a transfer map to cover our situation. The ring $P[\sqrt{d}]$ treated as a P-module is generated by two elements: 1, $\sqrt{d}$. Consider an P-module epimorphism $\Psi : P \times P \twoheadrightarrow P[\sqrt{d}]$ mapping $(x, y) \in P \times P$ to $x + y\sqrt{d}$. Thus we treat $P[\sqrt{d}]$ as a quotient module $P \times P/\ker\Psi$ of a free P-module of rank 2. Observe that $\ker\Psi = \{(-y\sqrt{d}, y) : y \in \mathfrak{c}\}$. Here $\mathfrak{c}$ denotes the *conductor* of the ring extension $P \subset P[\sqrt{d}]$, that is $\mathfrak{c} = \{a \in P : a \cdot P[\sqrt{d}] \subset P\} = \{a \in P : a \cdot \sqrt{d} \in P\}$. Being an ideal of P, the conductor is contained in $\mathfrak{m}$.

It is worth to identify the case when $P[\sqrt{d}]$ is a free P-module and so the standard definition of a transfer map holds:

Observation 2.8. *The ring $P[\sqrt{d}]$ is a free P-module with a basis $\{1, \sqrt{d}\}$ if and only if the conductor $\mathfrak{c}$ is null (i.e. $\mathfrak{c} = \{0\}$).*

Before we define the transfer map itself we need some preparatory steps. We define a family of epimorphisms of P-modules. Let $\Phi_1 : P[\sqrt{d}] \cong P \times P/\ker\Psi \twoheadrightarrow P/\mathfrak{c} \times P/\mathfrak{c}$ be given by $\Phi_1(x + y\sqrt{d}) := (x + \mathfrak{c}, y + \mathfrak{c})$ and $\Phi_n : P[\sqrt{d}]^n \twoheadrightarrow (P/\mathfrak{c})^{2n}$ for $n \geq 2$ be the associated epimorphisms of the product modules:

$$\Phi_n\bigl(\dots, x_i + y_i\sqrt{d}, \dots\bigr) := (\dots, x_i + \mathfrak{c}, y_i + \mathfrak{c}, \dots).$$

[1] An analogous obstacle obviously applies to higher degree extensions, as well. We simply do not need to formulate it here.

They are all well defined, since if $x+y\sqrt{d} = x'+y'\sqrt{d}$, then $(y'-y)\sqrt{d} = x-x' \in P$ and so $x-x', y-y' \in \mathfrak{c}$.

Observation 2.9. $\ker \Phi_1 = \{x + y\sqrt{d} \in P[\sqrt{d}] : x, y \in \mathfrak{c}\}$.

Lemma 2.10. *Let $\sigma \in \operatorname{Aut}_{P[\sqrt{d}]}\big(P[\sqrt{d}]^n\big)$ be an automorphism of a free $P[\sqrt{d}]$-module of rank n. If $U \in \ker \Phi_n$, then $\sigma(U) \in \ker \Phi_n$, as well.*

Proof. Let $U = \big(x_1 + y_1\sqrt{d}, \dots, x_n + y_n\sqrt{d}\big)$ and let $\big(a_{ij} + b_{ij}\sqrt{d}\big)_{1\le i,j\le n}$ be the matrix of σ (with respect to the canonical basis of $P[\sqrt{d}]^n$). Then

$$\begin{aligned}\sigma(U) &= \Big(\dots, \sum_{j=1}^n (a_{ij} + b_{ij}\sqrt{d})(x_j + y_j\sqrt{d}), \dots\Big)\\ &= \Big(\dots, \sum_{j=1}^n (a_{ij}x_j + b_{ij}y_j d) + \sum_{j=1}^n (a_{ij}y_j + b_{ij}x_j)\sqrt{d}, \dots\Big).\end{aligned}$$

All x_j, y_j belong to the conductor, since $U \in \ker \Phi_n$. Hence the sums are in the conductor, too. □

Lemma 2.11. *For every automorphism $\sigma \in \operatorname{Aut}_{P[\sqrt{d}]}\big(P[\sqrt{d}]^n\big)$ of a free $P[\sqrt{d}]$-module of rank n, there exists an associated automorphism $\overline{\sigma} \in \operatorname{Aut}_{P/\mathfrak{c}}(P/\mathfrak{c})^{2n}$ of a free $P/\mathfrak{c}$-module of rank $2n$ such that the following diagram commutes*

$$\begin{tikzcd} P[\sqrt{d}]^n \arrow[r, "\sigma"] \arrow[d, "\Phi_n"'] & P[\sqrt{d}]^n \arrow[d, "\Phi_n"] \\ (P/\mathfrak{c})^{2n} \arrow[r, "\overline{\sigma}"'] & (P/\mathfrak{c})^{2n} \end{tikzcd}$$

Proof. Define $\overline{\sigma} : (P/\mathfrak{c})^{2n} \to (P/\mathfrak{c})^{2n}$ by the formula

$$\overline{\sigma}\big(\Phi_n(U)\big) = \Phi_n\big(\sigma(U)\big).$$

First observe that $\overline{\sigma}$ is well defined. Indeed, if $\Phi_n(U) = \Phi_n(V)$ for any two vectors $U, V \in P[\sqrt{d}]^n$, then $U - V \in \ker \Phi_n$, hence by the previous lemma $\sigma(U - V) \in \ker \Phi_n$. Consequently $\Phi_n\big(\sigma(U)\big) = \Phi_n\big(\sigma(V)\big)$.

Next we show that $\overline{\sigma}$ is an endomorphism of a $P/\mathfrak{c}$-module. It is clear that $\overline{\sigma}$ is additive. Take now $x \in P$. Then

$$\overline{\sigma}\big(x \cdot \Phi_n(U)\big) = \overline{\sigma}\big(\Phi_n(xU)\big) = \Phi_n\big(\sigma(xU)\big) = x \cdot \Phi_n\big(\sigma(U)\big) = x \cdot \overline{\sigma}\big(\Phi_n(U)\big).$$

Hence $\overline{\sigma}$ is P-linear (and so is an endomorphism of an P-module $(P/\mathfrak{c})^{2n}$). It is also $P/\mathfrak{c}$-linear. Indeed, if $x + \mathfrak{c} = y + \mathfrak{c}$, then $x = y + c$ for some $c \in \mathfrak{c}$, hence

$$\overline{\sigma}\big(x \cdot \Phi_n(U)\big) = \overline{\sigma}\big((y + c) \cdot \Phi_n(U)\big) = y \cdot \overline{\sigma}\big(\Phi_n(U)\big) + c \cdot \overline{\sigma}\big(\Phi_n(U)\big) = y \cdot \overline{\sigma}\big(\Phi_n(U)\big).$$

Therefore, multiplication by elements of the quotient ring $P/\mathfrak{c}$ is well defined.

Take now any $V \in (P/\mathfrak{c})^{2n}$, there exists an element $U \in \big(P[\sqrt{d}]\big)^n$ such that $\Phi_n(U) = V$. Since σ is an automorphism of $\big(P[\sqrt{d}]\big)^n$, it follows that there is a vector $W \in \big(P[\sqrt{d}]\big)^n$ such that $\sigma(W) = U$. Thus $V = \Phi_n\big(\sigma(W)\big) = \overline{\sigma}\big(\Phi_n(W)\big)$. Consequently $\overline{\sigma}$ is an epimorphism.

Finally we prove that $\overline{\sigma}$ is a monomorphism. Suppose that $V = \Phi_n(U) \in \ker \overline{\sigma}$, hence $0 = \overline{\sigma}\big(\Phi_n(U)\big) = \Phi_n\big(\sigma(U)\big)$. Therefore $\sigma(U) \in \ker \Phi_n$. Thus by the previous lemma $U \in \ker \Phi_n$, as well. Consequently $V = 0$ in $(P/\mathfrak{c})^{2n}$. This proves that $\overline{\sigma}$ is an automorphism. □

We are now ready to define a transfer map in our set-up.

Definition 2.12. Let α, β be two arbitrary elements of the ring P. Denote by $s : P/\mathfrak{c} \times P/\mathfrak{c} \to P/\mathfrak{c}$ a homomorphism[2] $s(x, y) := x\alpha + y\beta$. For a bilinear form ξ on a free $P[\sqrt{d}]$-module of rank n we define a bilinear form $s_*\xi$ on a free $P/\mathfrak{c}$-module of rank $2n$ by the formula:

$$(s_*\xi)\big(\Phi_n(U), \Phi_n(V)\big) := (s \circ \Phi_1)\big(\xi(U, V)\big). \tag{2.1}$$

The previous lemmas show that $s_*\xi$ is well defined and if ξ, ζ are two bilinear forms over $P[\sqrt{d}]$ such that $\xi(U, V) = \zeta(\sigma(U), \sigma(V))$ for some automorphism σ, then

$$(s_*\xi)\big(\Phi_n(U), \Phi_n(V)\big) = (s_*\zeta)\big(\overline{\sigma}(\Phi_n(U)), \overline{\sigma}(\Phi_n(V))\big).$$

It follows from Observation 2.8, that this definition of a transfer map boils down to the traditional one, when $P[\sqrt{d}]$ is a free P-module.

Unfortunately, in general, $s_*\xi$ may be degenerate even when ξ is non-degenerate. Consequently, s_* does not need to induce a homomorphism between Witt groups of $P[\sqrt{d}]$ and $P/\mathfrak{c}$. We say that s_* is a *proper transfer* if it maps non-degenerate forms to non-degenerate form and hyperbolic to hyperbolic. In particular, if the above is the case, then s_* induces a group homomorphism $WP[\sqrt{d}] \to WP/\mathfrak{c}$, which (abusing the notation slightly) we again denote by s_*.

Let us introduce a useful matrix notation which is far easier to deal with than Eq. (2.1). Recall that $P[\sqrt{d}]$ is a local ring so every bilinear form over $P[\sqrt{d}]$ admits a diagonalization $\xi \cong \langle u_1, \dots, u_n \rangle$. The form ξ is non-degenerate if and only if $u_1, \dots, u_n$ are invertible by Corollary 1.5.

Proposition 2.13. *If $a + b\sqrt{d} \in P[\sqrt{d}]$ is invertible and $s : P/\mathfrak{c} \times P/\mathfrak{c} \to P/\mathfrak{c}$ is defined by $s(x, y) := x\alpha + y\beta$ for some $\alpha, \beta \in P$, then $s_*\langle a + b\sqrt{d}\rangle$ has a matrix representation*

$$\begin{pmatrix} a\alpha + b\beta & a\beta + b\alpha d \\ a\beta + b\alpha d & (a\alpha + b\beta)d \end{pmatrix} \tag{2.2}$$

Proof. Just expand Eq. (2.1) for $n = 1$ and $\xi = \langle a + b\sqrt{d}\rangle$. □

[2] Formally, $s(x + \mathfrak{c}, y + \mathfrak{c}) := (x\alpha + y\beta) + \mathfrak{c}$. In what follows we will abuse a notation writing x for $x + \mathfrak{c}$ when it is clear from a context that we are working in the quotient ring.

Corollary 2.14. *If* $\xi := \langle a_1 + b_1\sqrt{d}, \dots, a_n + b_n\sqrt{d}\rangle$ *is a diagonal bilinear form over* $P[\sqrt{d}]$, *then* $s_*\xi$ *is an orthogonal sum of forms given by Eq.* (2.2).

We will frequently refer to a transfer of a unit form $\langle 1\rangle$, hence it is convenient to write it down explicitly.

Corollary 2.15. *The transfer* $s_*\langle 1\rangle$ *is given by a matrix* $\left(\begin{smallmatrix}\alpha & \beta\\ \beta & \alpha d\end{smallmatrix}\right)$.

We are now ready to overcome the last obstacle in defining a transfer map, that is to describe all those s_* that map non-degenerate forms onto non-degenerate forms.

Proposition 2.16. *Let* $\alpha, \beta \in P$ *and* $s : P/\mathfrak{c} \times P/\mathfrak{c} \to P/\mathfrak{c}$ *be defined by* $s(x, y) := x\alpha + y\beta$, *then* s_* *is a proper transfer if and only if* β *is invertible modulo* $\mathfrak{c}$.

Proof. Clearly $\langle 1\rangle$ is a non-degenerate form. Compute the determinant of $s_*\langle 1\rangle$. It follows from Corollary 2.15 that $\det s_*\langle 1\rangle = \alpha^2 d - \beta^2$. Now $P/\mathfrak{c}$ is a local ring. Its maximal ideal is the image of $\mathfrak{m}$; denote it by $\overline{\mathfrak{m}}$. Since $\alpha^2 d \in \overline{\mathfrak{m}}$, hence $\alpha^2 d - \beta^2$ is invertible (and so $s_*\langle 1\rangle$ is non-degenerate) only when β is invertible in the quotient ring $P/\mathfrak{c}$.

Conversely suppose that β is invertible in P, hence also in $P/\mathfrak{c}$. Every bilinear form over $P[\sqrt{d}]$ is diagonalizable, since $P[\sqrt{d}]$ is local (c.f. Theorem 2.3). Thus all we have to do is to show that $s_*\langle a + b\sqrt{d}\rangle$ is non-degenerate for every invertible $a + b\sqrt{d} \in UP[\sqrt{d}]$. It follows from Eq. (2.2) that $s_*\langle a + b\sqrt{d}\rangle$ is given by the matrix

$$\begin{pmatrix} a\alpha + b\beta & a\beta + b\alpha d\\ a\beta + b\alpha d & (a\alpha + b\beta)d\end{pmatrix},$$

hence the determinant $\det s_*\langle a + b\sqrt{d}\rangle$ has a form

$$\det s_*\langle a + b\sqrt{d}\rangle = -a^2\beta^2 + \left(b^2\beta^2 + a^2\alpha^2 - b^2\alpha^2 d\right) \cdot d$$

The second term belongs to the maximal ideal $\overline{\mathfrak{m}}$ of $P/\mathfrak{c}$ while the first term is invertible because we assumed that $\beta \in U(P/\mathfrak{c})$ and a is invertible by Theorem 2.3. Consequently $\det s_*\langle a + b\sqrt{d}\rangle$ is invertible in $P/\mathfrak{c}$ and so $s_*\langle a + b\sqrt{d}\rangle$ is non-degenerate.

Observe that $s_*\langle -1\rangle$ has a matrix representation $\left(\begin{smallmatrix}-\alpha & -\beta\\ -\beta & -\alpha d\end{smallmatrix}\right)$, therefore $s_*\langle -1\rangle = -s_*\langle 1\rangle$. It follows that $s_*\langle 1, -1\rangle = \langle 1, -1\rangle$, hence s_* is proper. □

We can now give the first application of the theory developed so far. Until recently it was not known whether the Witt functor of the normalization of a Noetherian ring of dimension one must be an epimorphism. The only known result concerning this problem gives in fact an affirmative answer for orders in quadratic number fields (see [10]). The following theorem together with the subsequent propositions provides a family of counterexamples proving that this property does not hold in general.

Theorem 2.17. *Assume that there is $x \in P$ such that*

$$1 - x^2 d \notin (P/\mathfrak{c})^2, \tag{2.3}$$

then $W(P \rightarrowtail P[\sqrt{d}])$ is not an epimorphism.

Proof. Consider a functional $s : P/\mathfrak{c} \times P/\mathfrak{c} \to P/\mathfrak{c}$ given by $s(x, y) := y$ (i.e. $\alpha = 0$ and $\beta = 1$). Proposition 2.16 asserts that s_* is a proper transfer and so induces a group homomorphism $s_* : WP[\sqrt{d}] \to WP/\mathfrak{c}$ between the Witt groups. Take now any unit $u \in UP$. Then $s_*\langle u\rangle$ is associated with $\left(\begin{smallmatrix} 0 & u \\ u & 0 \end{smallmatrix}\right)$ and so hyperbolic over $P/\mathfrak{c}$, hence the composition $s_* \circ W(P \rightarrowtail P[\sqrt{d}])$ is null.

On the other hand $1+x\sqrt{d}$ is invertible in $P[\sqrt{d}]$ by Theorem 2.3 and $s_*\langle 1+x\sqrt{d}\rangle$ is given by

$$\begin{pmatrix} x & 1 \\ 1 & xd \end{pmatrix}.$$

Computing the determinant, we have $\det s_*\langle 1 + x\sqrt{d}\rangle = x^2 d - 1$. Hence, by the assumption on x, the form $s_*\langle 1 + x\sqrt{d}\rangle$ is not hyperbolic. Therefore the map $s_* : WP[\sqrt{d}] \to WP/\mathfrak{c}$ is not null. The composition

$$WP \xrightarrow{W(P \rightarrowtail P[\sqrt{d}])} WP[\sqrt{d}] \xrightarrow{s_*} WP/\mathfrak{c}$$

is thus the zero map but s_* itself is not. Consequently $W(P \rightarrowtail P[\sqrt{d}])$ cannot be an epimorphism. □

The assumption of the previous theorem are met in the case of real curve desingularization as the following proposition shows:

Proposition 2.18. *Let $\mathbb{k}$ be a real closed field and C a real algebraic curve over $\mathbb{k}$. Let further $P = R_\mathfrak{p}$ be a localization of the ring of functions regular on C at a singular point $\mathfrak{p} \in C$. If $\sqrt{d} \in \mathbb{k}(C)$, then there exists $x \in R_\mathfrak{p}$ satisfying Eq. (2.3).*

Proof. Let $\mathfrak{q}$ be a nonsingular real point of C but neither a zero nor a pole of d. The ring $R_\mathfrak{q}$ (i.e. the localization at $\mathfrak{q}$ of the ring of regular functions) is a valuation ring, since $\mathfrak{q}$ is nonsingular and so $R_\mathfrak{q}$ is integrally closed. It follows that $\sqrt{d} \in R_\mathfrak{q}$. The residue field of $R_\mathfrak{q}$ is $\mathbb{k}$ (because $\mathfrak{q}$ is real) and taking the value of d at $\mathfrak{q}$ we have

$$d(\mathfrak{q}) = \left(\sqrt{d}(\mathfrak{q})\right)^2 \in \mathbb{k}^2$$

and so $d(\mathfrak{q}) > 0$ in $\mathbb{k}$.

We shall consider two cases, when either $d(\mathfrak{q}) > 1$ or $d(\mathfrak{q}) < 1$ (if accidently $d(\mathfrak{q}) = 1$ we substitute $4d$ for d). In the first case, when $d(\mathfrak{q}) > 1$, take $x := 1$. Then $(1 - x^2 d)(\mathfrak{q}) < 0$ and so $1 - x^2 d$ is not a square. Conversely, assume $d(\mathfrak{q}) < 1$ and take x to be a constant function $x := \frac{1}{d(\mathfrak{q})} \in \mathbb{k}$. Then $(1 - x^2 d)(\mathfrak{q}) = 1 - \frac{1}{d(\mathfrak{q})} < 0$, hence again $1-x^2 d$ is not a square. In both cases x is a constant and so $x \in R_\mathfrak{p}$. □

2.2. Scharlau's norm principle

Original Scharlau's norm principle (see e.g. [33, Chapter VII, § 4]) describes the behavior of groups of similarity classes under a field extension. Here we prove an analogous result tailored for our specific needs. Recall that for a bilinear form ξ over a ring P, we denote $G_P(\xi)$ the *group of similarity factors* of ξ, this is:

$$G_P(\xi) := \{a \in UP : \langle a\rangle \otimes \xi \sim \xi\}.$$

In other words, $a \in G_P(\xi)$ if and only if a is invertible and $\langle 1, -a\rangle \otimes \xi$ is hyperbolic.

We keep the notation of previous sections concerning P and d. Moreover for $a+b\sqrt{d} \in P[\sqrt{d}]$ we write $N(a+b\sqrt{d})$ to denote the element $a^2-b^2d = \det\left(\begin{smallmatrix} a & bd \\ b & a\end{smallmatrix}\right) \in P/\mathfrak{c}$. It is well defined over $P/\mathfrak{c}$ (on the other hand it is possible that $N(a+b\sqrt{d})$ is not well defined over P). Indeed, if $a+b\sqrt{d} = a'+b'\sqrt{d}$, then $(b-b')\sqrt{d} = a'-a \in P$ and so both $a-a'$ and $b-b'$ belong to the conductor $\mathfrak{c}$. By an analogy to the field case, we call $N(a+b\sqrt{d})$ the *norm* of $a+b\sqrt{d}$. Further, for a diagonal form $\xi = \langle u_1, \ldots, u_n\rangle$ over P we denote by $\overline{\xi}$ a "reduced" form $\langle u_1+\mathfrak{c}, \ldots, u_n+\mathfrak{c}\rangle$ over $P/\mathfrak{c}$.

We shall prove the following version of Scharlau's Norm Principle

Theorem 2.19 ("Scharlau's Norm Principle"). *Let ξ be a bilinear form over P. For every $a+b\sqrt{d} \in UP[\sqrt{d}]$ the following implication holds:*

$$a+b\sqrt{d} \in G_{P[\sqrt{d}]}\bigl(\xi \otimes P[\sqrt{d}]\bigr) \implies N(a+b\sqrt{d}) \in G_{P/\mathfrak{c}}(\overline{\xi}).$$

Corollary 2.15 gives us an explicit matrix formula for a transfer of the unit form. However, to prove the theorem we would rather deal with diagonal forms (the ring $P/\mathfrak{c}$ is local, so every bilinear form over $P/\mathfrak{c}$ can be diagonalized). To this end we first prove the following lemmas:

Lemma 2.20 ([36, Corollary 2.2.9]). *Let $\langle u, v\rangle$ be a binary diagonal form over P and assume that it represents some $x \in UP$. Then $\langle u, v\rangle \cong \langle x, uvx\rangle$.*

Lemma 2.21. *Let $\alpha, \beta \in UP$ be two arbitrary units and let $s : P/\mathfrak{c} \times P/\mathfrak{c} \to P/\mathfrak{c}$ be defined by $s(x, y) := x\alpha + y\beta$. Then*

$$s_*\langle 1\rangle \cong \langle \alpha\rangle \otimes \langle 1, -N(\beta+\alpha\sqrt{d})\rangle.$$

Proof. By Corollary 2.15 we have $\det s_*\langle 1\rangle = \alpha^2 d - \beta^2 = -N(\beta+\alpha\sqrt{d})$. Hence, the determinants of $s_*\langle 1\rangle$ and $\langle \alpha\rangle \otimes \langle 1, -N(\beta+\alpha\sqrt{d})\rangle$ agree. It is easy to observe that the form $s_*\langle 1\rangle$ represents α. Therefore $s_*\langle 1\rangle \cong \langle \alpha, -\alpha \cdot N(\beta+\alpha\sqrt{d})\rangle$ by the previous lemma. □

Lemma 2.22. *Let $\alpha \in \mathfrak{m}$ be a noninvertible element and let $\beta \in UP$ be a unit. If s and s_* are defined as in the previous lemma, then*

$$s_*\langle 1\rangle \cong \langle 2\beta + (1+d)\alpha\rangle \otimes \langle 1, -N(\beta+\alpha\sqrt{d})\rangle.$$

Proof. This proof is fully analogous to the previous one. It is clear that determinants agree. Moreover, $s_*\langle 1\rangle$ represents $2\beta + (1+d)\alpha$ since

$$2\beta + (1+d)\alpha = (1,1)\begin{pmatrix}\alpha & \beta\\ \beta & \alpha d\end{pmatrix}\begin{pmatrix}1\\1\end{pmatrix}. \qquad \square$$

Proof of Theorem 2.19. Take a similarity factor $a + b\sqrt{d} \in G_{P[\sqrt{d}]}(\xi \otimes P[\sqrt{d}])$ of the form $\xi \otimes P[\sqrt{d}]$. Define $s : P/\mathfrak{c} \times P/\mathfrak{c} \to P/\mathfrak{c}$ by $s(x,y) := bx + ay$ (i.e. $\alpha = b$ and $\beta = a$ in the previous notation). It follows from Theorem 2.3 that a is a unit in P, since $a + b\sqrt{d} \in G_{P[\sqrt{d}]}(\xi \otimes P[\sqrt{d}]) \subset UP[\sqrt{d}]$. Hence, s_* is proper by Proposition 2.16. According to Eq. (2.2), for a unit $u \in P$, the matrix of $s_*\langle u \cdot (a + b\sqrt{d})\rangle$ has a form:

$$\begin{pmatrix} 2uab & u\cdot(a^2+b^2d)\\ u\cdot(a^2+b^2d) & 2uabd\end{pmatrix}.$$

Therefore, $\det s_*\langle u\cdot(a+b\sqrt{d})\rangle = -\big(u\cdot N(a+b\sqrt{d})\big)^2 \in -(U(P/\mathfrak{c}))^2$. Consequently $s_*\langle u \cdot (a + b\sqrt{d})\rangle$ is hyperbolic. It follows that $s_*\big((\langle -a - b\sqrt{d}\rangle \otimes \xi) \otimes P[\sqrt{d}]\big)$ is hyperbolic. On the other hand, the proceeding two lemmas assert that

$$s_*(\xi \otimes P[\sqrt{d}]) = \langle v\rangle \otimes \langle 1, -N(a + b\sqrt{d}\rangle \otimes \overline{\xi},$$

where v equals either b when b is invertible or $v = 2a + (1 + d)b$ when b is not invertible.

Consequently, we can write $s_*\big((\langle 1, -a - b\sqrt{d}\rangle \otimes \xi) \otimes P[\sqrt{d}]\big)$ as

$$\begin{aligned} s_*\Big((\langle 1, -a - b\sqrt{d}\rangle \otimes \xi) \otimes P[\sqrt{d}]\Big) &=\\ &= s_*\Big(\xi \otimes P[\sqrt{d}]\Big) \perp s_*\Big((\langle -a - b\sqrt{d} \otimes \xi\rangle) \otimes P[\sqrt{d}]\Big). \end{aligned}$$

The first term equals $\langle v\rangle \otimes \langle 1, -N(a + b\sqrt{d})\rangle \otimes \overline{\xi}$ while the second is hyperbolic. We assumed, that $a + b\sqrt{d}$ was a similarity factor of $\xi \otimes P[\sqrt{d}]$ and so $(\langle 1, -a - b\sqrt{d}\rangle \otimes \xi) \otimes P[\sqrt{d}]$ is hyperbolic. Consequently $\langle 1, -N(a+b\sqrt{d})\rangle \otimes \overline{\xi}$ is hyperbolic (over $P/\mathfrak{c}$). Thus $N(a + b\sqrt{d})$ is a similarity factor of $\overline{\xi}$. $\square$

As in the field case (c.f. [33, Corollary VII.4.4]) an immediate consequence of the previous theorem is the following:

Corollary 2.23. *Let ξ be a bilinear (non-degenerate) form over P. If it becomes hyperbolic over $P[\sqrt{d}]$ (i.e. $\xi \in \ker W(P \rightarrowtail P[\sqrt{d}])$), then $N(UP[\sqrt{d}]) \subset G_{P/\mathfrak{c}}(\overline{\xi})$.*

Another consequence of Scharlau's Norm Principle is the main theorem of this chapter. The reader may wish to compare it with Proposition 2.1.

Theorem 2.24. *Let P be a local ring and let $P \subset P[\sqrt{d}]$ be its non-unitary quadratic extensions.*

1. *The kernel of* $W(P \rightarrowtail P[\sqrt{d}])$ *does not contain any non-isotropic binary forms.*
2. *For every* $x \in P$ *the 2-fold Pfister form* $\langle\langle -1 - x^2d, -1 - x^2d\rangle\rangle$ *belongs to the kernel of the Witt functor* $W(P \rightarrowtail P[\sqrt{d}])$ *of this extension.*
3. *Let* $\mathfrak{c}$ *denote the conductor of this ring extension. The Witt functor* $W(P \twoheadrightarrow P/\mathfrak{c})$ *of the canonical epimorphism* $P \twoheadrightarrow P/\mathfrak{c}$ *maps the kernel of* $W(P \rightarrowtail P[\sqrt{d}])$ *into the intersection* $\bigcap_{x\in R} \operatorname{ann}\langle 1, -1 + x^2d\rangle$.

Proof. Suppose that $\langle a, b\rangle \in \ker W(P \rightarrowtail P[\sqrt{d}])$ for some $a, b \in UP$. This means that $\langle a, b\rangle \otimes P[\sqrt{d}]$ is hyperbolic and so $-ab$ is a square in $P[\sqrt{d}]$. Proposition 2.7 asserts that UP is quadratically closed and so $-ab$ is already a square in P. Consequently $\langle a, b\rangle$ is hyperbolic over P.

The inclusion $\{\langle\langle -1 - x^2d, -1 - x^2d\rangle\rangle : x \in P\} \cdot WP \subseteq \ker W(P \rightarrowtail P[\sqrt{d}])$ is clear since d is a square in $P[\sqrt{d}]$ and so $1+x^2d$ is a sum of two squares. Hence, the 2-fold Pfister form $\langle\langle -1-x^2d, -1-x^2d\rangle\rangle$ is isotropic and consequently hyperbolic (c.f. [36, Corollary 2.7.5]).

The last assertion follows from Scharlau's Norm Principle. Take any $\xi \in \ker W(P \rightarrowtail P[\sqrt{d}])$. Corollary 2.23 implies that $N(UP[\sqrt{d}]) \subset G_{P/\mathfrak{c}}(\bar{\xi})$. Theorem 2.3 describes $UP[\sqrt{d}]$, hence for every unit $a \in UP$ and every $b \in P$ we have

$$\langle a^2 - b^2d\rangle \otimes \bar{\xi} \sim \bar{\xi}.$$

Denote $x := {}^b/_a$; clearly x varies over all the elements of P when (a, b) varies over $UR \times P$. Thus, the form $\langle 1, -1 + x^2d\rangle \otimes \bar{\xi}$ is hyperbolic for every $x \in P$. □

Corollary 2.25. *If there is* $x \in P$ *such that* $1 + x^2d$ *is not a sum of two squares in* P*, then* $W(P \rightarrowtail P[\sqrt{d}])$ *is not a monomorphism.*

Proof. Suppose, a contrario, that $1 + x^2d$ is not a sum of two squares in P, but $\ker W(P \rightarrowtail P[\sqrt{d}])$ is nevertheless trivial. The Pfister form $\langle\langle -1-x^2d, -1-x^2d\rangle\rangle$ is hyperbolic by the previous theorem. It follows that $(1 + x^2d)\langle 1, 1\rangle \cong \langle 1, 1\rangle$, hence $1+x^2d$ is represented by the form $\langle 1, 1\rangle$ due to [36, Theorem 2.7.1], but this contradicts our assumptions. □

Appendix:
Unitary extensions of arbitrary degree

In this appendix we show that some of techniques developed in this chapter may be adapted to extensions of arbitrary degree, not only quadratic. The proofs presented below are quite sketchy, since they closely resemble the classical results known for fields. We use the following notation:

- P is a local domain in which 2 is invertible;
- $\mathfrak{m}$ is the maximal ideal of P;

- u is an integral element over P such that $u \in UP[u]$;
- $F \in P[T]$ is the minimal polynomial of u.

Take $k := P/\mathfrak{m}$ to be the residue field of P and let $k' := P[u]/\operatorname{Rad} P[u]$. Abusing the notation we use the overbar symbol to denote both canonical epimorphisms $P \twoheadrightarrow k$ and $P[u] \twoheadrightarrow k'$. Obviously $P[u]$ is a semi-local ring, hence using Chinese Reminder Theorem we see that k' is a product of fields (see also [36, Proposition II.1.3]).

Observation 2.26. *If $\mathfrak{m}_1, \dots, \mathfrak{m}_l$ are all the maximal ideals of $P[u]$, then*

$$k' \cong P[u]/\mathfrak{m}_1 \times \cdots \times P[u]/\mathfrak{m}_l.$$

We treat k' as an k-algebra.

Lemma 2.27. *The k-algebra k' has a basis of the form $\{1, \overline{u}, \dots, \overline{u}^{N-1}\}$ for some $N \leq \deg F$.*

Proof. Since the elements $1, u, \dots, u^{\deg F-1}$ generate $P[u]$ as a P-module, thus the set $\{1, \overline{u}, \dots, \overline{u}^{\deg F-1}\}$ generates k' as a k-linear space. We construct a basis of k' starting from $\{1\}$ and appending the consecutive powers of $\overline{u}$ as long as the set remains linearly independent. Suppose that the process stopped after N steps, so we constructed a linearly independent set $\mathscr{B} = \{1, \overline{u}, \dots, \overline{u}^{N-1}\}$ and $\overline{u}^N \in \operatorname{lin} \mathscr{B}$. Thus

$$\overline{u} = \sum_{i=0}^{N-1} x_i \overline{u}^i$$

for some $x_0, \dots, x_{N-1} \in k$. The next power of $\overline{u}$ can be written as

$$\overline{u}^{N+1} = \overline{u} \cdot \overline{u}^N = \sum_{i=1}^{N-1} x_{i-1} \overline{u}^i + \sum_{i=0}^{N-1} x_{N-1} x_i \overline{u}^i \in \operatorname{lin} \mathscr{B}.$$

We inductively prove that all the remaining generators of k' sit in $\operatorname{lin} \mathscr{B}$. Therefore $\mathscr{B}$ is a basis of k'. □

In what follows, N will always denote the dimension of k' over k. As in the case of non-unitary quadratic extensions, we investigate $W(P \rightarrowtail P[u])$ using an appropriately defined transfer. As before, the problem occurs when $P[u]$ is not a free P-module[3].

Take a k-linear map $s : k' \to k$. The ring $P[u]$ is semi-local, hence any bilinear form over $P[u]$ admits a diagonalization (see Proposition 1.7). Take a form $\xi = \langle v_1, \dots, v_n \rangle$ over $P[u]$ with $v_1, \dots, v_n \in UP[u]$. Let $\overline{\xi} = \langle \overline{v_1}, \dots, \overline{v_n} \rangle$ denote its *reduction* to k'. Finally, let $s_* \overline{\xi} : ({k'}^n \times {k'}^n) \otimes k' \to k$ be the bilinear form over k obtained by taking the composition $s \circ \overline{\xi}$.

[3] In fact, if $P[u]$ is free over P, the ring extension $P \subset P[u]$ is étale and the Witt functor $W(P \rightarrowtail P[u])$ has already been described in the literature, see [42] and [58].

Definition 2.28. We say that s_* is a *proper transfer*, if $s_*\overline{\xi}$ defined above is non-degenerate for every non-degenerate bilinear form ξ over $P[u]$ and s_* maps hyperbolic forms to hyperbolic forms.

Observation 2.29. *If s_* is a proper transfer, then s_* induces a homomorphism of Witt groups $WP[u] \to Wk$ which (abusing the notation slightly) we again denote by s_*.*

Lemma 2.30. *If $s \in \operatorname{Hom}_k(k', k)$ gives rise to a proper transfer s_*, then for every unit $v \in Uk'$ a map $t : k' \to k$ defined by $t(x) := s(vx)$ gives rise to a proper transfer t_*.*

Proof. Take a non-degenerate bilinear form ξ over $P[u]$. Then its reduction $\overline{\xi}$ is again non-degenerate. We are working over a field now, hence it suffices to show that the null vector is the only one orthogonal to the whole space. Take a non-zero vector $W \in k'^n \otimes k$. By the assumption, s_* is proper, so there exists another vector V such that $(s_*\overline{\xi})(W, V) \neq 0$. Taking $V' := v^{-1}V$ we have $(t_*\overline{\xi})(W, V') = s(vv^{-1}\overline{\xi}(W, V)) \neq 0$. $\square$

Lemma 2.31. *Take a k-linear map $s : k' \to k$ defined on the basis $\{1, \overline{u}, \ldots, \overline{u}^{N-1}\}$ by the formula*

$$s(\overline{u}^i) := \begin{cases} 0, & \text{if } 0 \leq i < N-1, \\ 1, & \text{if } i = N-1. \end{cases}$$

Then s_* is a proper transfer.

Proof. Take any non-zero vector $w \in k'^n \otimes k$. As $w \neq 0$, there exists a map $\varphi \in \operatorname{Hom}(k'^n, k')$ such that $\varphi(w) \neq 0$.The form $\overline{\xi}$ is non-degenerate since ξ is non-degenerate by the assumption. Hence, there is a vector $v \in k'^n$ such that $\varphi = \overline{\xi}(v, \cdot)$. In particular, $\overline{\xi}(v, w) = \varphi(w) \neq 0$. Suppose $\overline{\xi}(v, w) = x_0 + x_1\overline{u} + \cdots + x_k\overline{u}^m$ with $x_m \neq 0$, thus

$$\overline{\xi}(\overline{u}^{N-m-1} \cdot v, w) = x_0\overline{u}^{N-m-1} + x_1\overline{u}^{N-m} + \cdots + x_m\overline{u}^{N-1}.$$

Consequently $(s_*\overline{\xi})\big(\overline{u}^{N-m-1}v, w\big) = x_m \neq 0$, which means that $\overline{u}^{N-m-1}v$ and w are not orthogonal. $\square$

Corollary 2.32. *For every $j \in \{0, \ldots, N-1\}$ the map $s_j : k' \to k$ defined by*

$$s_j(\overline{u}^i) := \begin{cases} 0, & \text{if } i \neq j, \\ 1, & \text{if } i = j. \end{cases}$$

gives rise to a proper transfer $(s_j)_*$.

Lemma 2.33. *Suppose that s is defined as in Lemma 2.31, if the dimension $N = \dim_k k'$ is even, then the composition $s_* \circ W(P \rightarrowtail P[u])$ is null.*

Proof. The ring P is local and so every bilinear form over P has a diagonalization. Consequently, we need only to prove that for every unary form $\langle v\rangle$ over P, the form $\xi := s_*\big(\overline{\langle v\rangle \otimes P[u]}\big)$ is hyperbolic. To this end, consider a subspace U of $(k'\otimes k, \xi)$ spanned by $1, \overline{u}, \dots, \overline{u}^{N/2-1}$ (recall that N is the dimension of k' over k). Observe that U is totally isotropic. Indeed, for any $X = x_0 + x_1\overline{u} + \dots + x_{N/2-1}\overline{u}^{N/2-1}$ and $Y = y_0 + y_1\overline{u} + \dots + y_{N/2-1}\overline{u}^{N/2-1}$ we have

$$\xi(X,Y) = s(\overline{v}XY) = s\big(\overline{v}x_0y_0 + \overline{v}x_0y_1 + \dots + \overline{v}x_{N/2-1}y_{N/2-1}\overline{u}^{N-2}\big) = 0.$$

It follows from [33, Theorem I.3.4 (1)] that $s_*\big(\overline{\langle v\rangle \otimes P[u]}\big)$ is hyperbolic. □

Now, let $(\alpha_0, \alpha_1, \dots, \alpha_{N-1})$ be the coordinates of $\overline{u}^N$ with respect to the basis $\{1, \overline{u}, \dots, \overline{u}^{N-1}\}$. Then $f := \alpha_0 + \alpha_1 T + \ldots + \alpha_{N-1}T^{N-1} + T^N \in k[T]$ can be viewed as a minimal polynomial of $\overline{u}$ over k. However, in general, since k' is not necessarily a field, f may be reducible. The reader may wish to compare the following proposition with Theorem 2.17

Proposition 2.34. *If the dimension $N = \dim_k k'$ is even and the constant term α_0 of f is not a minus square in k, then the Witt class of $\langle u\rangle$ does not belong to the image of $W(P \rightarrowtail P[u])$. In particular $W(P \rightarrowtail P[u])$ is not surjective.*

Proof. Let $s : k' \to k$ be defined as in Lemma 2.31, compute the transfer $s_*\langle\overline{u}\rangle$. Proceeding as in the previous proof, we show the subspace of $(k'\otimes k, s_*\langle\overline{u}\rangle)$ spanned by $1, \overline{u}, \dots, \overline{u}^{(N-1)/2}$ is totally isotropic. Hence using [33, Theorem I.3.4 (1)] we can split a hyperbolic subspace of dimension $N-2$ out of $(k'\otimes k, s_*\langle\overline{u}\rangle)$. Thus we write

$$s_*\langle\overline{u}\rangle \cong \big(\tfrac{N}{2} - 1\big)\langle 1, -1\rangle \perp \text{binary form}.$$

Compute the determinant $\det s_*\langle\overline{u}\rangle = (-1)^{N/2-1}\alpha_0$. It follows that $s_*\langle\overline{u}\rangle$ is not hyperbolic since α_0 is not a minus square in k by the assumption. □

Suppose now that the field k can be embedded into the local ring P. Let $s : k' \to k$ be a linear map inducing a proper transfer $s_* : WP[u] \to Wk$, such that $s_*\langle 1\rangle = \langle 1\rangle$. Consider the following maps:

$$0 \rightleftarrows \ker s_* \underset{\tau}{\overset{i}{\rightleftarrows}} WP[u] \underset{j}{\overset{s_*}{\rightleftarrows}} Wk \rightleftarrows 0,$$

where i is the canonical inclusion, $j = W(k \rightarrowtail P[u])$ is induced by the embedding $k \rightarrowtail P$ and τ is defined by the formula $\tau(\xi) := \xi - (j\circ s_*)(\xi)$.

Proposition 2.35. *With the above notation:*

1. *the sequence $0 \to \ker s_* \to WP[u] \to Wk \to 0$ is exact;*
2. *the sequence $O \leftarrow \ker s_* \leftarrow WP[u] \leftarrow Wk \leftarrow 0$ is a complex (i.e. $\tau\circ j = 0$);*
3. *$\tau \circ i = \mathrm{id}_{\ker s_*}$;*

4. $s_* \circ j = \mathrm{id}_{Wk}$;
5. $\ker s_*$ *is generated (as a group) by the set* $\{\langle v\rangle - (j \circ s_*)\langle v\rangle : v \in UP[u]\}$.

Proof. The first assertion is trivial, the second follows immediately from the forth. Take any $\xi \in \ker s_*$, then

$$(\tau \circ i)(\xi) = \xi - (j \circ s_*)(\xi) = \xi - j(0) = \xi,$$

which proves point (2.35). Next, take any $\xi = \langle w_1, \dots, w_n\rangle \in Wk$, then $j\xi = \langle w_1, \dots, w_n\rangle \otimes P[u]$. Since, we assumed that $s_*\langle 1\rangle = \langle 1\rangle$, it follows that $s_*\langle w_i\rangle = w_i \cdot s_*\langle 1\rangle = \langle w_i\rangle$ and so $(s_* \circ j)(\xi) = \xi$. This proves point (2.35). The last assertion follows immediately. $\square$

Corollary 2.36. *Under the above assumptions* $WP[u] \cong \ker s_* \oplus Wk$.

3

Injectivity of Witt functor of ring normalization

Let us begin with the following very simple, nevertheless motivating, observation.

Observation 3.1. *Let $P \subset R$ be an arbitrary ring extension. If there is a unit $u \in UP$ such that u is a square in R but not in P, then the bilinear form $\langle u, -1\rangle$ is hyperbolic in R but not in P. In particular $W(P \rightarrowtail R)$ is not a monomorphism.*

The most natural case is the one when $R = \operatorname{int.cl.} P$ is the *integral closure* of P. One starts wonder how important is the fact that u is invertible. As we shall see this condition is not necessary. It was proved in [12, Theorem 5.1] that if there is $x \in R \setminus P$ such that both x^2 and $2x$ sit in P, then $W(P \rightarrowtail R)$ is not a monomorphism. This condition cannot, however, be satisfied when 2 is invertible, what we always assume. Hence, the pursuit for properties of a ring P that prevent the Witt functor to map the inclusion $P \rightarrowtail \operatorname{int.cl.} P$ to a monomorphism is the leading theme of this chapter. The first part of this chapter is devoted to the proof of Theorem 3.15 asserting that the Witt functor of normalization of a seminormal ring that is not quadratically closed is noninjective. In fact we prove an even stronger result (see Theorem 3.11) that locally unitary quadratic extensions cause the Witt functor of the normalization to be noninjective. The assumptions of this theorem are expressed in terms of elements of the ring and its normalization. This is, however, not very convenient, since it is well known that the arithmetic of an arbitrary ring (even a normal ring like $\operatorname{int.cl.} P$ not to mention P itself) can be very complicated. Far easier objects to study than elements of a ring are its ideals. Hence, the second part of this chapter explores a relationship between the Picard functor and the Witt functor of ring normalization (see Theorem 3.24). Finally, at the appendix we present an application of this theory to the desingularization of a real algebraic curve.

3.1. Preparatory lemmas

We gather here some basic lemmas which are needed later. Some of them are probably well known, but lacking a convenient source of reference, we have included their proofs for the sake of completeness. In what follows, for an ideal I of a ring P and a prime $\mathfrak{p} \in \operatorname{Spec} P$, we denote $I_\mathfrak{p} := I \cdot P_\mathfrak{p}$ the localization of I at $\mathfrak{p}$.

LEMMA 3.2. *Let P be an integral domain and $I \lhd P$ an ideal, then I is the intersection of all its localizations, i.e.:*

$$I = \bigcap_{\mathfrak{p} \in \operatorname{Spec} P} I_\mathfrak{p}.$$

Proof. Of course I is contained in its localization $I_\mathfrak{p}$ for every prime $\mathfrak{p}$, hence one inclusion is obvious and we need to prove only the other one. Take an element x of the right hand side intersection. For any prime ideal $\mathfrak{p} \in \operatorname{Spec} P$ we write $x = {}^{a_\mathfrak{p}}/_{b_\mathfrak{p}} \in I_\mathfrak{p}$ for some $a_\mathfrak{p} \in I$ and $b_\mathfrak{p} \in P \setminus \mathfrak{p}$. Let J denote the ideal of P generated by the set $\{b_\mathfrak{p} : \mathfrak{p} \in \operatorname{Spec} P\}$. Then J is not contained in any prime of P, hence $J = P$ is the improper ideal, in particular $1 \in J$. Thus, there are $t_1, \dots, t_k \in P$ such that $1 = t_1 b_{\mathfrak{p}_1} + \cdots + t_k b_{\mathfrak{p}_k}$. Multiplying by x we have $x = t_1 a_{\mathfrak{p}_1} + \cdots + t_k a_{\mathfrak{p}_k}$ and so $x \in I$. $\square$

The following observation is a special case of [1, Exercise 1.18], we write it down explicitely for an easy reference.

OBSERVATION 3.3. *Let P be a ring, $I \lhd P$ an ideal and $\mathfrak{p} \in \operatorname{Spec} P$ a prime of P. Then the square of the localization of I equals the localization of the square of I, i.e. $(I_\mathfrak{p})^2 = (I^2)_\mathfrak{p}$.*

In what follows we will write in short $I^2_\mathfrak{p}$ since the meaning is clear due to the previous observation.

LEMMA 3.4. *Let $P \subsetneq R$ be two integral domains with the same field of fractions and let $I \lhd P$ be an ideal. If I is projective as a P-module, then $IR \not\subset I$.*

It is a know fact, that an ideal is projective if and only if it is invertible (see e.g. [32, Theorem 2.17]). The following proof of the lemma, actually incorporates a part of a proof of this assertion.

Proof. Express I as an image of some free P-module M by an epimorphism $\varphi : M \twoheadrightarrow I$. By the assumption, I is projective, hence φ splits. Let $\psi : I \rightarrowtail M$ be such that $\varphi \circ \psi = \mathrm{id}_I$. Fix a basis $\{\varepsilon_j\}_{j \in J}$ of M and denote π_j the projection on j-th coordinate, i.e. $\pi_j(\sum_{j \in J} x_j \varepsilon_j) := x_j$. Further, let ψ_j be the composition $\psi_j := \pi_j \circ \psi \in \operatorname{Hom}_P(I, P)$. Observe that for every $x \in I$, we have $\psi(x) = \sum_{j \in J} \psi_j(x) \varepsilon_j$. Consequently, $\psi_j(x)$ is null for all but finitely many $j \in J$.

Let N be the submodule of $\operatorname{Hom}_P(I, P)$ spanned by the set $\{\psi_j : j \in J\}$. We claim that $N(I) = P$. The inclusion $N(I) \subseteq P$ is obvious. For the other inclusion, fix any non-zero $x \in I$ and take $a \in P$. The element x is invertible in the field of fractions $K := \operatorname{qf}(P)$. Let J_0 be the (finite) set of all the indexes j for which $\psi_j(xa) \neq 0$. We have

$$a = \frac{1}{x}\varphi\big(\psi(xa)\big) = \frac{1}{x}\varphi\Big(\sum_{j\in J_0}\psi_j(xa)\varepsilon_j\Big) = \sum_{j\in J_0} a\psi_j\big(\varphi(\varepsilon_j)\big) \in N(I).$$

This proves our claim.

Suppose, a contrario to the assertion, that $IR \subseteq I$. Take any $\sum_{j\in J_0} c_j\psi_j \in N$ for some finite set of indexes $J_0 \subset J$ and let $x \in I$ and $a \in R$, then

$$\Big(\sum_{j\in J_0} c_j\psi_j(x)\Big)\cdot a = \sum_{j\in J_0} c_j\psi_j(ax) \in N(I).$$

It follows that

$$R = P\cdot R = N(I)\cdot R \subseteq N(I) = P,$$

which contradicts our assumption. □

We shall need the following theorem of R. Parimala and R. Sridharan to prove the lemma following it.

THEOREM 3.5 ([43, Theorem 3.1]). *Let P be a Noetherian domain of dimension 1. If the singular locus of P is finite but not empty, then every bilinear form (M,ξ) over P, such that $(M,\xi)\otimes P_{\mathfrak{p}}$ contains a hyperbolic plane for every singular prime $\mathfrak{p}$, contains a hyperbolic subspace of rank 2.*

We present here two applications of the above result. Recall (see Proposition 1.13) that a module $I\oplus P$ admits a bilinear form when I^2 is principal.

LEMMA 3.6. *Let P be a Noetherian domain of dimension 1 and let $I \lhd P$ be an ideal such that $I^2 = d\cdot P$. If a bilinear module $(I\oplus P,\xi)$ is hyperbolic, where the form ξ is defined by $\xi(x\oplus y, x'\oplus y') := \frac{1}{d}xx' - yy'$, then d is a square in P. The opposite implication is also true providing that P has only finitely many singular primes.*

Proof. Suppose that d is not a square in P. Let K be the field of fractions of P. The form $(I\oplus P,\xi)\otimes K = \langle {}^1\!/_d, -1\rangle$ is hyperbolic over K. It follows that d is a square in the field of fractions of P and so $\sqrt{d} = {}^a\!/_b$ for some $a,b\in P$, $b\neq 0$.

Since $(I\oplus P,\xi)$ is hyperbolic, it follows that there is a direct summand N of $I\oplus P$ satisfying $N = N^\perp$. It is straightforward to check that N must coincide with exactly one of the two sets:

$$\big\{x\oplus y \in I\oplus P : x = y\sqrt{d}\big\}, \qquad \big\{x\oplus y\in I\oplus P : x = -y\sqrt{d}\big\}, \tag{3.1}$$

as these are the only two totally isotropic submodules of $I\oplus P$.

Consider a homomorphism $\lambda : N \to P$ of P-modules defined by the formula $\lambda(x\oplus y) := bx$. Observe that λ is a monomorphism. Indeed, take $x\oplus y\in N$ such that $\lambda(x\oplus y) = bx = 0$. The ring P is integral and so $x = 0$. Now $x\oplus y \in N = N^\perp$, hence $x\oplus y$ is strongly isotropic. Computing ξ on this vector we have

$$0 = \xi(x \oplus y, x \oplus y) = \frac{1}{d}x^2 - y^2.$$

Consequently $x^2 = dy^2$ and so $y = 0$ as well.

Take now $N' := \operatorname{im}\lambda$. It is an ideal of P isomorphic as a P-module to N. For any $bx \in N'$, we have $bx \cdot \sqrt{d} = ax \in P$. Therefore N' is contained in the conductor $\mathfrak{c}$ of the ring extension $P \subsetneq P[\sqrt{d}]$. Observe that N' is simultaneously an ideal of both P and $P[\sqrt{d}]$. Indeed, if $bx \in N'$, then there is $y \in P$ such that $x \oplus y \in N$. It follows from Eq. (3.1), that $x = y\sqrt{d}$ (the second case, when $x = -y\sqrt{d}$ is fully analogous). Hence $bx\sqrt{d} = byd$. But $yd \oplus x$ lies again in N, consequently $bx\sqrt{d} \in N'$. Therefore $N' \cdot P[\sqrt{d}] = N'$. It follows from Lemma 3.4 that N' is not projective. Consequently N itself is not projective but this contradicts our assumption that N is a direct summand of $I \oplus P$.

The opposite implication follows from Theorem 3.5. If P does not have any singular primes, then it is a Dedekind domain and $W(P \rightarrowtail K)$ is a monomorphism by Knebusch-Milnor Theorem, hence $(I \oplus P, \xi)$ is hyperbolic over P because it is hyperbolic over its field of fractions. Now suppose that P is not Dedekind. Since d is a square in P, so it is a square in every localization of P. Therefore $(I \oplus P, \xi)_{\mathfrak{p}} \cong (P_{\mathfrak{p}}^2, \langle \frac{1}{d}, -1\rangle)$ is hyperbolic for every prime $\mathfrak{p}$ of P. Thus $(I \oplus P, \xi)$ is hyperbolic by Theorem 3.5. □

We can now formulate a sufficient local condition for the Witt functor of a ring normalization to be injective (or equivalently a necessary condition for it being noninjective).

Proposition 3.7. *Let P be a Noetherian domain of dimension one with a finite singular locus. If $W(P_{\mathfrak{p}} \rightarrowtail \operatorname{int.cl.} P_{\mathfrak{p}})$ is a monomorphism for every prime $\mathfrak{p}$ of P, then $W(P \rightarrowtail \operatorname{int.cl.} P)$ is a monomorphism.*

Proof. If P does not have any singular primes, then P is a Dedekind ring and so the assertion is vacuously true. Thus we assume that the singular locus of P is non-empty. Denote by $R := \operatorname{int.cl.} P$ the integral closure of P. If $W(P \rightarrowtail R)$ is noninjective, then there exists a non-hyperbolic bilinear space (M, ξ) over P such that its extension $(M, \xi) \otimes R$ is hyperbolic. Theorem 3.5 asserts that there is a prime $\mathfrak{p}$ of P such that $(M, \xi) \otimes P_{\mathfrak{p}}$ is not hyperbolic. Take $\mathfrak{P}$ to be a prime of R lying over $\mathfrak{p}$. Clearly $(M, \xi) \otimes R_{\mathfrak{P}}$ is hyperbolic. The integral closure of $P_{\mathfrak{p}}$ is a Dedekind domain. It follows from Theorem 1.40 that $W(\operatorname{int.cl.} P_{\mathfrak{p}} \rightarrowtail R_{\mathfrak{P}})$ is a monomorphism. Observe that $W(P_{\mathfrak{p}} \rightarrowtail \operatorname{int.cl.} P_{\mathfrak{p}})$ is not injective. Indeed, if $W(P_{\mathfrak{p}} \rightarrowtail \operatorname{int.cl.} P_{\mathfrak{p}})$ was injective, then $W(P_{\mathfrak{p}} \rightarrowtail R_{\mathfrak{P}})$ would be injective, as well. But this is clearly impossible as $(M, \xi) \otimes P_{\mathfrak{p}}$ is non-hyperbolic, while $(M, \xi) \otimes R_{\mathfrak{P}}$ is hyperbolic. □

3.2. Locally unitary quadratic extensions

In this chapter we are trying to identify those rings for which normalization is not mapped to a monomorphism by the Witt functor. Observe that if we can factor the normalization $P \rightarrowtail \operatorname{int.cl.} P$ through an auxiliary ring R:

$$P \rightarrowtail R \rightarrowtail \operatorname{int.cl.} P$$

in such a way that already $W(P \rightarrowtail R)$ is not a monomorphism, then $W(P \rightarrowtail \operatorname{int.cl.} P)$ is not a monomorphism, either. Our motivating Observation 3.1 suggests that we should take R to be a quadratic extension $R = P[\sqrt{d}]$ for some carefully selected d. This is exactly what we do in this section.

The following lemma may seem rather technical, but it will turn out to be an indispensable ingredient of the proof of our main theorem.

Lemma 3.8. *Let P be a Noetherian domain of dimension 1 and let R be an integrally closed domain finite over P. Suppose that there exists $d \in P$ which is not a square in P but is a square in R. Let J be the principal ideal generated by $\sqrt{d}$ in some subring $Q \subseteq R$ containing $\sqrt{d}$ (i.e. $P[\sqrt{d}] \subseteq Q \subseteq R$ and $J = \sqrt{d} \cdot Q$) and let $I = J \cap P$ be the contraction of J. If I^2 is principal generated by d, then $W(P \rightarrowtail R)$ is not a monomorphism.*
Moreover, if P has only finitely many singular primes, then the assumption that R is integrally closed may be omitted.

Proof. Consider a projective P-module $M := I \oplus P$. It follows from Proposition 1.13 that one can define a bilinear form on M. Let $\xi : M \times M \to P$ be given by the formula

$$\xi(x \oplus y, x' \oplus y') := \frac{1}{d} xx' - yy'.$$

Then (M, ξ) is non-degenerate by Proposition 1.15 and it is not hyperbolic by Lemma 3.6. On the other hand, $(M, \xi) \otimes K = (K^2, \langle ({}^1/\!\sqrt{d})^2, -1\rangle)$ is clearly hyperbolic over $K := \operatorname{qf}(R)$ the field of fractions of R. Now R is a Dedekind domain, thus $W(R \rightarrowtail K)$ is a monomorphism by Theorem 1.40. It follows that $(M, \xi) \otimes R$ is hyperbolic, hence the Witt class of (M, ξ) is in the kernel of $W(P \rightarrowtail R)$ which cannot, thus, be a monomorphism.

As for the moreover part, observe that if P has only finitely many singular primes so does Q. It follows from Lemma 3.6 that $(M, \xi) \otimes Q$ is hyperbolic. Thus neither $W(P \rightarrowtail Q)$ nor $W(P \rightarrowtail R)$ is a monomorphism. $\square$

Lemma 3.9. *Let P be an integral domain. Suppose that $d \in P$ is not a square. Denote $J := \sqrt{d} \cdot P[\sqrt{d}]$ an ideal of $P[\sqrt{d}]$ and let $I := J \cap P$ be the contraction of J. Fix a prime $\mathfrak{p}$ of P and a prime $\mathfrak{P}$ of $P[\sqrt{d}]$ lying over $\mathfrak{p}$. If the local ring $P_{\mathfrak{p}}$ contains $\sqrt{d}$, then the localization $I_{\mathfrak{p}}$ of I is principal and*

$$I_{\mathfrak{p}} = \sqrt{d} \cdot P_{\mathfrak{p}} = J_{\mathfrak{P}} \cap P_{\mathfrak{p}}.$$

Proof. The ring $P[\sqrt{d}]$ is a P-module and P, J are its submodules. Localization commutes with module intersection by [1, Corollary 3.5], therefore

$$I_\mathfrak{p} = (J \cap P) \cdot P_\mathfrak{p} = J \cdot P_\mathfrak{p} \cap P \cdot P_\mathfrak{p} = J \cdot P_\mathfrak{p} = \sqrt{d} \cdot P[\sqrt{d}] \cdot P_\mathfrak{p} = \sqrt{d} \cdot P_\mathfrak{p}.$$

The last equation follows from the assumption that $\sqrt{d} \in P_\mathfrak{p}$. Thus we proved that $I_\mathfrak{p} = \sqrt{d} \cdot P_\mathfrak{p}$ is principal. What is left, is to show that $I_\mathfrak{p}$ is actually the contraction of $J_\mathfrak{P}$.

Observe that [1, Proposition 1.17.i] provides one inclusion, namely $I_\mathfrak{p} = J \cdot P_\mathfrak{p} \subset J_\mathfrak{P} \cap P_\mathfrak{p}$. To prove the other one, notice that $J_\mathfrak{P} = J \cdot P[\sqrt{d}]_\mathfrak{P} = \sqrt{d} \cdot P[\sqrt{d}]_\mathfrak{P}$ is principal. Take an element $a \cdot \sqrt{d} \in J_\mathfrak{P} \cap P_\mathfrak{p}$ where a is a fraction $(x + y\sqrt{d})/(x' + y'\sqrt{d}) \in P[\sqrt{d}]_\mathfrak{P}$ with $x + y\sqrt{d} \in J \subset P[\sqrt{d}]$ and $x' + y'\sqrt{d} \in P[\sqrt{d}] \setminus \mathfrak{P}$. Then both elements $x + y\sqrt{d}$ and $x' + y'\sqrt{d}$ are contained in $P_\mathfrak{p}$ since $\sqrt{d} \in P_\mathfrak{p}$ by the assumption. Moreover $P_\mathfrak{p}$ is a local ring and $x' + y'\sqrt{d} \notin \mathfrak{p} \cdot P_\mathfrak{p}$, it follows that $x' + y'\sqrt{d}$ is invertible in $P_\mathfrak{p}$. All in all $a = (x + y\sqrt{d})/(x' + y'\sqrt{d}) \in P_\mathfrak{p}$ and consequently $x \cdot \sqrt{d} \in \sqrt{d} \cdot P_\mathfrak{p} = I_\mathfrak{p}$. □

We shall say that a quadratic extension $P \subset P[\sqrt{d}]$, where $d \in P$ is not a square, is *locally unitary* if $P_\mathfrak{p} \subset P_\mathfrak{p}[\sqrt{d}]$ is unitary for every prime $\mathfrak{p} \in \operatorname{Spec} P$. This is equivalent to the the condition that for every prime ideal $\mathfrak{p} \in \operatorname{Spec} P$ if $d \in \mathfrak{p}$ then $\sqrt{d} \in P_\mathfrak{p}$.

Lemma 3.10. *Let P be a Noetherian domain of dimension one and let $P \subsetneq P[\sqrt{d}]$ be a locally unitary quadratic extension such that $P[\sqrt{d}]$ has the same field of fractions as P. Further let $J := \sqrt{d} \cdot P[\sqrt{d}]$ be an ideal of $P[\sqrt{d}]$ and $I := J \cap P$ be its contraction. Then $I^2 = d \cdot P$ is a principal ideal.*

Proof. Let $\mathfrak{c} = \{x \in P : x\sqrt{d} \in P\}$ be the conductor of the ring extension $P \subset P[\sqrt{d}]$. Take any $a, b \in I = J \cap P$. Since J is principal generated by $\sqrt{d}$ we can express a and b as:

$$\begin{aligned} a &= \big(x + y\sqrt{d}\big) \cdot \sqrt{d} = x\sqrt{d} + yd, \\ b &= \big(x' + y'\sqrt{d}\big) \cdot \sqrt{d} = x'\sqrt{d} + y'd, \end{aligned}$$

for some $x, x', y, y' \in P$. Both a and b belong to P so do yd and $y'd$. Consequently $x, x' \in \mathfrak{c}$. Computing the product $a \cdot b$ we have

$$a \cdot b = \big(xx' + (x'\sqrt{d})y + (x\sqrt{d})y' + yy'd\big) \cdot d.$$

Every term of the sum in the parenthesis lies in P, hence $ab \in d \cdot P$. This proves the inclusion $I^2 \subset dP$.

We shall now prove the opposite inclusion. It suffices to show that $d \in I^2$. Using Lemma 3.2 and Observation 3.3 we have

$$I^2 = \bigcap_{\mathfrak{p} \in \operatorname{Spec} P} I_\mathfrak{p}^2.$$

Thus, we need to show that $d \in I_{\mathfrak{p}}^2$ for every $\mathfrak{p}$ of P. Consider the three possible cases:

- $\mathfrak{p}$ is a regular prime,
- $\mathfrak{p}$ is a singular prime and $d \in \mathfrak{p}$,
- $\mathfrak{p}$ is a singular prime and $d \notin \mathfrak{p}$,

First suppose that $\mathfrak{p}$ is regular and so $P_{\mathfrak{p}}$ is a valuation ring. In particular, $P_{\mathfrak{p}}$ is normal, therefore $\sqrt{d} \in P_{\mathfrak{p}}$. It follows from Lemma 3.9 that $I_{\mathfrak{p}} = \sqrt{d} \cdot P_{\mathfrak{p}}$ hence $d \in I_{\mathfrak{p}}^2$. Suppose now that $\mathfrak{p}$ is a singular prime such that $d \in \mathfrak{p}$. Thus, d is not invertible in $P_{\mathfrak{p}}$, it follows that $\sqrt{d} \in P_{\mathfrak{p}}$ since $P \subset P[\sqrt{d}]$ is locally unitary by the assumptions. Using Lemma 3.9 again, we have $I_{\mathfrak{p}} = \sqrt{d} \cdot P_{\mathfrak{p}}$ hence $d \in I_{\mathfrak{p}}^2$. Finally suppose that $\mathfrak{p}$ is singular and $d \notin \mathfrak{p}$. Therefore d is a unit of $P_{\mathfrak{p}}$, hence $I_{\mathfrak{p}}$ is the improper ideal of $P_{\mathfrak{p}}$ and so $I_{\mathfrak{p}}^2 = P_{\mathfrak{p}}$. Thus again $d \in I_{\mathfrak{p}}^2$. □

Combining the previous three lemmas together we prove that if there is a quadratic locally unitary sub-extension of the normalization of P, then the Witt functor of the normalization is not a monomorphism.

THEOREM 3.11. *Let P be a Noetherian domain of dimension 1 and let R be its integral closure. If there exists $d \in P$ not a square such that d is a square in R and the ring extension $P \subset P[\sqrt{d}]$ is locally unitary, then the Witt functor $W(P \rightarrowtail R)$ of the normalization of P is not a monomorphism.*
The class of $\big((\sqrt{d} \cdot R \cap P) \oplus P, \langle \frac{1}{d}, -1\rangle\big)$ is an explicit non-trivial element of the kernel $W(P \rightarrowtail R)$.
Moreover, if P has only finitely many singular primes, then the assumption that $R = \operatorname{int.cl.} P$ may be weakened to $R \subseteq \operatorname{int.cl.} P$.

The assumption that there is a quadratic locally unitary sub-extension of a normalization is not completely intuitive, neither it is easy to check for an arbitrary domain. In the next section we will substitute it with a simpler condition concerning the Picard functor of this normalization. First, however, we show how it relates to the standard notion of seminormality.

The *Picard group* of a commutative ring P is the set of isomorphism classes of line bundles over P with the group operation induced by the tensor product. We denote this group by $\operatorname{Pic} P$. The assignment $P \mapsto \operatorname{Pic} P$ is a covariant functor from the category of commutative rings to the category of abelian groups called the *Picard functor*. For details see e.g. [32, §20].

Recall (see e.g. [56]) that a finite ring extension R of a domain P is called *subintegral* if the following two conditions are satisfied:

- for every prime $\mathfrak{p}$ of P, there exists exactly one prime $\mathfrak{P}$ of R lying over $\mathfrak{p}$,
- the canonical homomorphism of the residue fields $\operatorname{qf}(P/\mathfrak{p})$ and $\operatorname{qf}(R/\mathfrak{P})$ is an isomorphism.

The maximal subintegral extension of P contained within its field of fractions is called the *seminormalization* of P. The ring P is *seminormal* if it is equal to its seminormalization. We have the following characterization of seminormal rings:

Traverso-Swan Theorem 3.12 ([8, Proposition 4.67 and Theorem 4.74]). *Let P be a domain and K its field of fractions. The following conditions are equivalent:*

1. *P is seminormal,*
2. $\operatorname{Pic} P = \operatorname{Pic} P[T_1, \dots, T_n]$ *for every $n \in \mathbb{N}$,*
3. *for every $t \in K$, if $t^2, t^3 \in P$ then also $t \in P$.*

Using the last condition, it is straightforward to show that seminormality is a local property (see also [8, Proposition 4.66]):

Observation 3.13. *If P is a commutative ring, then the following conditions are equivalent:*

1. *P is seminormal,*
2. *$P_{\mathfrak{m}}$ is seminormal for every maximal ideal $\mathfrak{m}$ of P,*
3. *$P_{\mathfrak{p}}$ is seminormal for every prime ideal $\mathfrak{p}$ of P.*

We formulate yet another criterion of seminormality.

Proposition 3.14. *Let P be a Noetherian domain of dimension 1. Then P is seminormal if and only if for every $\beta \in \operatorname{int.cl.} P$ such that $\beta^2 \in P$ the ring extension $P \subset P[\beta]$ is locally unitary.*

Proof. Assume that P is seminormal. Fix an element $\beta \in \operatorname{int.cl.} P$ such that β^2 lies in P. Of course, if β itself belongs to P, then $P \subset P[\beta]$ is trivially locally unitary. Hence we assume that β does not belong to P. Take a prime $\mathfrak{p}$ of P and suppose that the extension $P_{\mathfrak{p}} \subset P_{\mathfrak{p}}[\beta]$ of the local rings is not unitary. Theorem 2.3 asserts that $P_{\mathfrak{p}}[\beta]$ is a local ring. In particular, the only maximal ideal of $P_{\mathfrak{p}}$ extends uniquely to $P_{\mathfrak{p}}[\beta]$. Moreover, the residue fields of $P_{\mathfrak{p}}$ and $P_{\mathfrak{p}}[\beta]$ are canonically isomorphic by Observation 2.4. It follows that $P_{\mathfrak{p}}[\beta]$ is a subintegral extension of $P_{\mathfrak{p}}$ and so $P_{\mathfrak{p}}$ is not a seminormal ring contrary to the previous observation.

We now prove the opposite implication. Suppose that P is not seminormal. It follows from Traverso-Swan Theorem that there is $\beta \in \operatorname{int.cl.} P$ such that $\beta^2, \beta^3 \in P$ but $\beta \notin P$. Using Lemma 3.2 we can write

$$P = \bigcap_{\mathfrak{p} \in \operatorname{Spec} P} P_{\mathfrak{p}}$$

and so β^2 and β^3 belong to every localization of P but there is a prime $\mathfrak{p} \in \operatorname{Spec} P$ such that $\beta \notin P_{\mathfrak{p}}$. The extension $P_{\mathfrak{p}} \subsetneq P_{\mathfrak{p}}[\beta]$ is unitary, hence β^2 is invertible in $P_{\mathfrak{p}}$. Thus $\beta = \beta^3 \cdot (\beta^2)^{-1} \in P_{\mathfrak{p}}$—contradiction. □

We can now present an easier-to-digest (but weaker) consequence of Theorem 3.11.

THEOREM 3.15. *If P is a seminormal Noetherian domain,* $\dim P = 1$*, which is not quadratically closed in its integral closure R, then $W(P \to R)$ is not a monomorphism.*

3.3. Relations to the Picard functor

Arithmetic of an arbitrary ring can be quite complex. It is far easier to work with ideals of a ring than its elements. In fact, this is why ideals were invented in the first place. In this section we show that existence of 2-torsions in the kernel of the Picard functor of the normalization of a ring P forces the Witt functor of this normalization to be non-injective (see Theorem 3.11). First we recall the Mayer-Vietoris sequence for Picard groups. Let $P \subset R$ be two domains with the same field of fractions and such that R is a finitely generated P-module (we say that R is *finite over* P). Denote by $\mathfrak{c}$ the conductor of the ring extension $P \subset R$. In what follows, $\overline{u}$ denotes the coset $u + \mathfrak{c}$ of an element u. Consider the following commutative diagram, where the horizontal arrows are the embeddings and the vertical ones are the canonical epimorphisms:

$$\begin{tikzcd} P \arrow[r, tail] \arrow[d, two heads] & R \arrow[d, two heads] \\ P/\mathfrak{c} \arrow[r, tail] & R/\mathfrak{c}. \end{tikzcd}$$

It gives raise to the following group homomorphisms:

- $\varPhi : UP \to UR \oplus U(P/\mathfrak{c})$, sending $\varPhi(u) = (u, \overline{u})$;
- $\Psi : UR \oplus U(P/\mathfrak{c}) \to U(R/\mathfrak{c})$, mapping $\Psi(u, \overline{v}) = {}^{\overline{u}}/_{\overline{v}}$;
- $\Lambda : \operatorname{Pic} P \to \operatorname{Pic} R \oplus \operatorname{Pic} P/\mathfrak{c}$, defined as

$$\Lambda(M) = (M \otimes_P R, M \otimes_P P/\mathfrak{c}) \cong (MR, \overline{M});$$

- $\Xi : \operatorname{Pic} R \oplus \operatorname{Pic} P/\mathfrak{c} \to \operatorname{Pic} R/\mathfrak{c}$, given by

$$\Xi(M, \overline{N}) = (M \otimes_R R/\mathfrak{c}) \otimes_{R/\mathfrak{c}} \overline{N}^{-1}.$$

THEOREM 3.16. *Using the above notation, if $P \subset R$ are two domains with the same field of fractions and R is finite over P, then there is a group homomorphism* $\Delta : U(R/\mathfrak{c}) \to \operatorname{Pic} P$ *such that the following sequence is exact:*

$$1 \to UP \xrightarrow{\varPhi} UR \oplus U(P/\mathfrak{c}) \xrightarrow{\Psi} U(R/\mathfrak{c}) \xrightarrow{\Delta}$$
$$\xrightarrow{\Delta} \operatorname{Pic} P \xrightarrow{\Lambda} \operatorname{Pic} R \oplus \operatorname{Pic} P/\mathfrak{c} \xrightarrow{\Xi} \operatorname{Pic} R/\mathfrak{c}.$$

For the proof see either [57, Theorem 3.10] or [3, Theorem IX.5.3 and Example IX.5.6] In fact, it can be shown (for details see [57]) that $\Delta(\overline{u})$ is the class of a P-module $M_u := \{(x, \overline{y}) \in R \times P/\mathfrak{c} : \overline{ux} = \overline{y}\}$. If we factor the last term of this sequence (i.e. $\operatorname{Pic} R/\mathfrak{c}$) by itself and push it back through the sequence forcing Λ to become an epimorphism, we arrive at another version of the sequence (which can be proved constructively, see [35]).

THEOREM 3.17 ([35, Theorem 7]). *Let P, R, $\mathfrak{c}$ be as in Theorem 3.16 and assume that* $\dim P = 1$. *The following sequence is exact:*

$$1 \to UR/UP \xrightarrow{\psi} U(R/\mathfrak{c})/U(P/\mathfrak{c}) \xrightarrow{\delta} \operatorname{Pic} P \xrightarrow{\lambda} \operatorname{Pic} R \to 1,$$

where the group homomorphisms are defined as follows:

- $\psi(u) = \overline{u}$;
- $\delta(u) = uP + \mathfrak{c}$;
- $\lambda(M) = MR$.

For the rest of this section we silently keep the assumptions as in the above theorem. Observe that by mapping $(x, \overline{y})$ to ux we define an isomorphism between M_u and $uR \cap P$. Therefore we have (see also [57, Exercise 3.9]):

OBSERVATION 3.18. *For every $u \in R$ invertible modulo $\mathfrak{c}$, the P-modules M_u and $uR \cap P$ are isomorphic.*

It is convenient to write the relations between the two above exact sequences explicitely.

PROPOSITION 3.19. *The following diagram is commutative with exact diagonals:*

$$\begin{tikzcd}
U(R/\mathfrak{c}) \arrow[rr, two heads, "\overline{u} \mapsto \overline{u}^{-1}"] \arrow[dr, "\overline{u} \mapsto M_u"'] & & U(R/\mathfrak{c})/U(P/\mathfrak{c}) \arrow[dl, "\overline{u} \mapsto uP + \mathfrak{c}"] \\
& \operatorname{Pic} P \arrow[dl, "M \mapsto MR"'] \arrow[dr, "M \mapsto (MR, \overline{M})"] & \\
\operatorname{Pic} R & & \operatorname{Pic} R \oplus \operatorname{Pic} P/\mathfrak{c} \arrow[ll, two heads, "M \hookleftarrow\!\mapsto (M, N)"]
\end{tikzcd}$$

Proof. The exactness of diagonals follows from theorems 3.16 and 3.17. It is clear that the lower triangle commutes. All we have to do is to prove that the upper one commutes, as well. Take any $u \in R$ invertible in $R/\mathfrak{c}$. Let $v \in R$ be its inverse modulo $\mathfrak{c}$, this means that $c := uv - 1$ belongs to the conductor $\mathfrak{c}$. We claim that the P-modules $uR \cap P$ and $vP + \mathfrak{c}$ are isomorphic. Consider a map f that sends $x \in vP + \mathfrak{c}$ to $ux \in uR \cap P$. We can write $x = v \cdot a + c'$ for some $a \in P$ and $c' \in \mathfrak{c}$. Therefore

$$ux = uva + uc' = (c + 1) \cdot a + uc' \in P.$$

Clearly, ux belongs to uR and so ux sits in $uR \cap P$. The map f is a monomorphism of P-modules. It is also an epimorphism because, if $y = ux \in uR \cap P$, then $y = f(v \cdot y + (-x) \cdot c) \in f(vP + \mathfrak{c})$. □

Let us write down one more helpful fact:

Observation 3.20 ([35, Proposition 2]). *For any $u \in R$ invertible modulo $\mathfrak{c}$, the P-module $uP + \mathfrak{c}$ is principal if and only if there is a unit $v \in UR$ such that $uv \in P$.*

We note some consequences:

Lemma 3.21. *Keep the above notation. Let N be an element of the kernel of $\operatorname{Pic}(P \rightarrowtail R)$ having order two in the Picard group $\operatorname{Pic} P$ of P. Then there exists such an element $\beta \in R$ that:*

1. *$N \cong \beta R \cap P$;*
2. *β is invertible modulo $\mathfrak{c}$ and if γ is its inverse modulo $\mathfrak{c}$ (i.e. $\beta\gamma - 1 \in \mathfrak{c}$), then the P-modules M_β and M_γ are isomorphic;*
3. *$\beta \cdot UR$ is disjoint with P;*
4. *there is a unit $u \in UR$ such that $\beta^2 u \in P$.*

Proof. We assume that $N \in \ker \operatorname{Pic}(P \rightarrowtail R) = \ker \lambda$, hence Theorem 3.17 asserts that $N \cong \beta P + \mathfrak{c}$ for some β such that $\overline{\beta} \in U(R/\mathfrak{c})/U(P/\mathfrak{c})$. It follows from Proposition 3.19 and Observation 3.18 that $N \cong M_\gamma \cong \gamma R \cap P$. In the Picard group $\operatorname{Pic} P$ we have $N^2 = 1$ and so $N = N^{-1}$. Now $\Delta : U(R/\mathfrak{c}) \to \operatorname{Pic} P$ is a homomorphism, therefore $M_\beta = \Delta(\beta) = \Delta(\gamma^{-1}) = N^{-1} = N = M_\gamma$. This proves assertions (3.21) and (3.21). The remaining assertion (3.21) and (3.21) follow from the preceding observation. □

Proposition 3.22. *Keep the above notation, let N, β be defined as in Lemma 3.21 and let u be a unit of R such that $\beta^2 u \in P$. Then the quadratic ring extension $P[u] \subset P[u, \beta]$ is locally unitary.*

Proof. Suppose that $P[u] \subset P[u, \beta]$ is not locally unitary. Thus there is a prime $\mathfrak{p}$ of $P[u]$ such that the ring extension $P[u]_\mathfrak{p} \subsetneq P[u]_\mathfrak{p}[\beta]$ is not unitary. This means that $\beta \notin P[u]_\mathfrak{p}$ and β is not a unit in $P[u]_\mathfrak{p}[\beta]$. It follows from Theorem 2.3, that $P[u]_\mathfrak{p}[\beta]$ is a local ring, hence $\mathfrak{P} := \mathfrak{p} \cdot P[u]_\mathfrak{p}[\beta]$ is its unique maximal ideal consequently $\beta \in \mathfrak{P}$.

Denote by $\mathfrak{c}_0$, $\mathfrak{c}_1$ and $\mathfrak{c}_2$ the conductors of the ring extension respectively $P \subset R$, $P[u] \subset R$ and $P[u]_\mathfrak{p} \subset P[u]_\mathfrak{p}[\beta]$. It is obvious that $\mathfrak{c}_0 \subseteq \mathfrak{c}_1$. We claim that the extension $\mathfrak{c}_1 \cdot P[u]_\mathfrak{p}$ of $\mathfrak{c}_1$ is fully contained in $\mathfrak{c}_2$. Indeed, take any $c \in \mathfrak{c}_1$ and

$s \in P[u] \setminus \mathfrak{p}$. Then $c\beta \in P[u]$ consequently $\frac{c\beta}{s} \in P[u]_{\mathfrak{p}}$. Now, $\mathfrak{c}_2$ is a proper ideal, since β does not belong to $P[u]_{\mathfrak{p}}$. Hence $\mathfrak{c}_2$ is contained in the maximal ideal of $P[u]_{\mathfrak{p}}[\beta]$ that we have denoted by $\mathfrak{P}$ above. On the other hand, β is invertible modulo $\mathfrak{c}_0$ (see Lemma 3.21(3.21)). Therefore, there exists $\gamma \in R$ such that $\beta\gamma - 1 \in \mathfrak{c}_0 \subset \mathfrak{c}_2 \subset \mathfrak{P}$. This is impossible since β belongs to $\mathfrak{P}$. □

We shall need the following simple consequence of the Lying-Over Theorem (c.f. [1, Theorem 5.10]). We write it down explicitly to provide a convenient reference.

Observation 3.23. *If $P \subset R$ is an integral ring extension, then every element $x \in P$ which is invertible in R is already invertible in P.*

Theorem 3.24. *Let P be a Noetherian domain of dimension 1 and let $R = \operatorname{int.cl.} P$ be its integral closure. Suppose that $UR \subset P$. If the kernel of $\operatorname{Pic}(P \rightarrowtail R)$ contains an element of order 2, then $W(P \rightarrowtail R)$ is not a monomorphism. Moreover, if P has only finitely many singular primes, then the assumption that $R = \operatorname{int.cl.} P$ may be weakened to $R \subseteq \operatorname{int.cl.} P$.*

Proof. By the previous proposition $P = P[u] \subsetneq P[\beta]$ is a locally unitary quadratic extension with $\beta \in R \setminus P$ and $\beta^2 \in P$. Thus the assertion follows from Theorem 3.11. □

Remark 3.25. Observe that the assumption $UP = UR$ of the previous theorem means that the first term of the exact sequence in Theorem 3.17 disappeares, and so the Picard functor of the normalization $P \rightarrowtail R$ is described by the following short exact sequence:

$$1 \to U(R/\mathfrak{c})/U(P/\mathfrak{c}) \to \operatorname{Pic} P \to \operatorname{Pic} R \to 1.$$

Appendix: Curve desingularization

In this section we show how to aply the results of previous sections to curve normalization. Namely, we consider the following situation: let $\Bbbk$ be a fixed field of characteristic $\operatorname{char} \Bbbk \neq 2$ (later we will assume that $\Bbbk$ is a real closed field). Take a (singular) curve C over $\Bbbk$ and let $\hat{C}$ be its smooth model. We thus have a normalization morphism $\pi : \hat{C} \twoheadrightarrow C$ and an associated embedding of the coordinate rings $\Bbbk[C] \rightarrowtail \Bbbk[\hat{C}] = \operatorname{int.cl.} \Bbbk[C]$. We study the Witt functor of this embedding $W(\Bbbk[C] \rightarrowtail \Bbbk[\hat{C}])$ in terms of the singularity type of C.

The simplest singular curve is a cubic one. Recall (see e.g. [7, § 7.3]) that over the reals there are exactly three classes of singular irreducible cubic curves with respect to the projective equivalence. These are (see Figure 3.1):

- acnodal curves, represented by $y^2 + x^3 + x^2 = 0$;
- crunodal curves, represented by $y^2 - x^3 - x^2 = 0$;

- cuspidal curves, represented by $y^2 - x^3 = 0$.

The affine classification of singular cubics is more complex even over the reals, not to mention other ground fields (like e.g. the rationals). We shall not cope with this issue here, though, and concentrate only on the above three types, as this suffices to illustrate how our methods work.

PROPOSITION 3.26. *Let $\mathbb{k}$ be a field of characteristic* $\operatorname{char}\mathbb{k} \neq 2$ *and such that* -1 *is not a square in* $\mathbb{k}$. *Let* $P = \mathbb{k}[x,y]/(y^2 + x^3 + x^2)$ *be the coordinate ring of an acnodal cubic over* $\mathbb{k}$. *Then the Picard group of* P *is* $\operatorname{Pic} P \cong \mathbb{k}(\sqrt{-1})^*/\mathbb{k}^*$*, the normalization* $P \subset \operatorname{int.cl.} P$ *is a locally unitary quadratic extension and so the Witt functor* $W(P \rightarrowtail \operatorname{int.cl.} P)$ *of the normalization is not a monomorphism.*

Proof. Denote the integral closure of P by R. It is easy to show that $R = P[y/x] \cong \mathbb{k}[t]$ since the smooth model of the acnodal cubic is obtained by a single blow-up. Next, the conductor of the normalization is $\mathfrak{c} = xP + yP$. Consequently $P/\mathfrak{c} \cong \mathbb{k}$ and $R/\mathfrak{c} \cong \mathbb{k}(\sqrt{-1})$. Moreover $UR = UP = \mathbb{k}^*$, therefore it follows from Theorem 3.17 that $\operatorname{Pic} P \cong \mathbb{k}(\sqrt{-1})^*/\mathbb{k}^*$.

The class of $\sqrt{-1}$ has order two in the group $\mathbb{k}(\sqrt{-1})^*/\mathbb{k}^*$. Thus there exists an element of order 2 in the kernel of $\operatorname{Pic}(P \rightarrowtail R)$, consequently $W(P \rightarrowtail R)$ is not injective by Theorem 3.24. □

Remark 3.27. In fact a non-trivial element in the kernel of $W(P \rightarrowtail \operatorname{int.cl.} P)$ can be explicitly constructed as follows. Write the ring P as $P = \mathbb{k}[x, x\sqrt{-x-1}]$. The integral closure of P (denote it R again) is then $R = \mathbb{k}[x, \sqrt{-x-1}]$. Take J to be the principal ideal of R generated by $\sqrt{-x-1}$ and let $I := J \cap P$ be its contraction. One checks that I is not principal but I^2 is principal, namely $I^2 = (x+1) \cdot P$—for reader's convenience in Figure 3.2 we provide an explicit Macaulay-2 (see [18]) code, in case $\mathbb{k} = \mathbb{Q}$. By means of Lemma 3.8. we can construct a bilinear form ξ on $I \oplus P$ such that $(I \oplus P, \xi)$ is not hyperbolic while $(I \oplus P, \xi) \otimes R$ is hyperbolic.

PROPOSITION 3.28. *Let $\mathbb{k}$ be a field of characteristic* $\operatorname{char}\mathbb{k} \neq 2$ *and let* $P = \mathbb{k}[x,y]/(y^2 - x^3 - x^2)$ *be the coordinate ring of a crunodal curve over* $\mathbb{k}$. *Then the Picard group of* P *is* $\operatorname{Pic} P \cong \mathbb{k}^*$*, the normalization* $P \subset \operatorname{int.cl.} P$ *is locally unitary and so the Witt functor* $W(P \rightarrowtail \operatorname{int.cl.} P)$ *of the normalization is not a monomorphism.*

The proof is fully analogous to the previous one and so we skip it. The two above propositions concern *any* field (of characteristic $\neq 2$). If we narrow our focus to a specific category of fields, much more can be said. If the field $\mathbb{k}$ is real closed, the following theorem of J.-P. Monnier gives an explicit description of the Witt groups involved.

THEOREM 3.29 ([40, Theorem 3.10]). *Let $\mathbb{k}$ be a real closed field and C an integral affine curve over $\mathbb{k}$, $C(\mathbb{k})$ the set of real points of C, $\pi : \hat{C} \twoheadrightarrow C$ the normalization of C and S the singular locus. Denote the number of real and complex points of*

S (respectively $\pi^{-1}(S)$) by y_r, y_c (resp. $\hat{y}_r$, $\hat{y}_c$). Further let s be the number of semi-algebraic connected components of $C(\Bbbk)$, g the genus of smooth completion of $\hat{C} \otimes \Bbbk(\sqrt{-1})$ and r (resp. c) the number of real (resp. complex) points needed to make $\hat{C}$ complete.

1. *If both $C(\Bbbk)$ and $\hat{C}(\Bbbk)$ are non-empty, then*
$$WC \cong \mathbb{Z}^s \oplus (\mathbb{Z}/2\mathbb{Z})^{g+c+(\hat{y}_c-y_c)+(\hat{y}_r-y_r)}.$$
2. *If $C(\Bbbk) \neq \varnothing$ but $\hat{C}(\Bbbk) = \varnothing$ and $\hat{C} \otimes \Bbbk(\sqrt{-1})$ is connected, then*
$$WC \cong \mathbb{Z}^s \oplus (\mathbb{Z}/2\mathbb{Z})^{g+c+(\hat{y}_c-y_c)-y_r}.$$
3. *If $C(\Bbbk) \neq \varnothing$ and $\hat{C} \otimes \Bbbk(\sqrt{-1})$ is not connected, then*
$$WC \cong \mathbb{Z}^{y_r} \oplus (\mathbb{Z}/2\mathbb{Z})^{2g+c+(\hat{y}_c-y_c)-y_r-1}.$$
4. *If $C(\Bbbk) = \varnothing$ and both $C \otimes \Bbbk(\sqrt{-1})$ and $\hat{C} \otimes \Bbbk(\sqrt{-1})$ are connected, then*
$$WC \cong (\mathbb{Z}/4\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z})^{g+c+(\hat{y}_c-y_c)-2}.$$
5. *If $C(\Bbbk) = \varnothing$, $C \otimes \Bbbk(\sqrt{-1})$ is connected but $\hat{C} \otimes \Bbbk(\sqrt{-1})$ is not connected, then*
$$WC \cong (\mathbb{Z}/4\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z})^{2g+c+(\hat{y}_c-y_c)-2}.$$
6. *If $C(\Bbbk) = \varnothing$ and both $C \otimes \Bbbk(\sqrt{-1})$ and $\hat{C} \otimes \Bbbk(\sqrt{-1})$ are not connected, then*
$$WC \cong (\mathbb{Z}/2\mathbb{Z})^{2g+c+(\hat{y}_c-y_c)}.$$

In this special case the two preceding propositions can be easily derived from the above theorem as follows. For an acnodal real curve we have:
$$s = 2,\ y_r = 1,\ y_c = 0,\ \hat{y}_r = 0,\ \hat{y}_c = 1,\ g = 0,\ r = 1,\ c = 0.$$
Thus Theorem 3.29 asserts that $WP \cong \mathbb{Z}^2$ while $WR \cong \mathbb{Z}$ and so clearly $W(P \rightarrowtail R)$ cannot be a monomorphism. Similarly, for a crunodal curve we have:
$$s = 1,\ y_r = 1,\ y_c = 0,\ \hat{y}_r = 2,\ \hat{y}_c = 0,\ g = 0,\ r = 1,\ c = 0.$$
It follows from Theorem 3.29 that $WP \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ and so $W(P \rightarrowtail R)$ is not a monomorphism, either. On the other hand, for a cuspidal curve we have
$$s = 1,\ y_r = 1,\ y_c = 0,\ \hat{y}_r = 1,\ \hat{y}_c = 0,\ g = 0,\ r = 1,\ c = 0.$$
Using Theorem 3.29 again we have $WP \cong \mathbb{Z}$. Consequently $W(P \rightarrowtail R)$ is an isomorphism!

We observed above that the coordinate ring of a cubic curve with an ordinary multiple point admits more orthogonal geometries than its normalization. This is a more general phenomenon. For an integral real curve C denote by $R = R(C)$ the ring of functions regular in every real point of C.

Proposition 3.30. *Let $\Bbbk$ be a real closed field. If C is a singular real curve over $\Bbbk$ having an ordinary multiple point with real tangents, then the Witt functor $W(R(C) \rightarrowtail \operatorname{int.cl.} R(C))$ of normalization of the ring $R(C)$ of functions regular on C is not a monomorphism.*

Proof. The proposition can be proved using Theorem 3.29 and its complete counterpart [40, Theorem 3.9] scrutinously counting numbers of components and real/complex singularities of a curve before and after it was blown-up in the style of XIX century algebraic geometry. There is however a simpler proof.

Without loss of generality, we may assume that the multiple point lies at the origin of an affine plane $\mathbb{A}^2(\Bbbk) \subset \mathbb{P}^2(\Bbbk)$ and $\{X = 0\}$ is not a tangent at the origin. The exceptional divisor of the blow-up of C intersects the proper transform (denote it $\hat{C}$) at n distinct points $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ (since the origin was an ordinary multiple point). Let $t_1 < \cdots < t_n$ denote the ordinates of these intersection points. Take m to an even number $m \geq n$ and take $a_0, \dots a_{m-1} \in \Bbbk$ to be a solution of the following system of linear equations

$$\begin{cases} a_{m-1}t_1^{m-1} + \cdots + a_1 t_1 + a_0 = (-1)^1 \\ a_{m-1}t_2^{m-1} + \cdots + a_1 t_2 + a_0 = (-1)^2 \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ a_{m-1}t_n^{m-1} + \cdots + a_1 t_n + a_0 = (-1)^n \end{cases}$$

Consider a rational function $g \in \Bbbk(T)$ given by the formula

$$g := \frac{1}{T^m + 1}\bigl(T^m + a_{m-1}T^{m-1} + \cdots + a_1 T + a_0\bigr)$$

and take $G \in \Bbbk(\hat{C})$ to be the function on $\hat{C}$ such that

$$G\,\big|_{\mathbb{A}^2(\Bbbk)\cap\hat{C}}\,(x, y) = g(y).$$

It is clear that G is regular on $\hat{C}$ since $\lim_{t\to\pm\infty} g(t) = 1$. On the other hand $G(\mathfrak{p}_i) = (-1)^i$ for $1 \leq i \leq n$ and so G is not regular on C (near the origin, on some of the branches of G converges to 1, while on the others it converges to -1). At the same time G^2 is regular at the origin and consequently everywhere on C.

All in all, we found an element $G \in \Bbbk(\hat{C}) = \Bbbk(C)$ such that $G \notin R(C)$ but $G^2 \in R(C)$. Moreover, the ring $\bigl(R(C)\bigr)(G)$ has exactly two points $\mathfrak{q}_1$, $\mathfrak{q}_2$ lying over the origin separated by G (i.e. $G(\mathfrak{q}_1) = -1$ while $G(\mathfrak{q}_2) = 1$). It follows from Theorem 2.3 that the ring extension $R(C) \subsetneq \bigl(R(C)\bigr)(G)$ is locally unitary. Thus the Witt functor of the normalization of $R(C)$ is not a monomorphism by Theorem 3.11. □

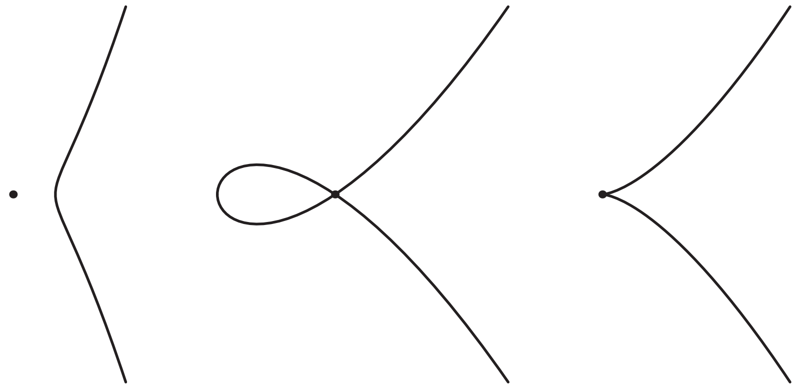


Figure 3.1. Acnodal, crunodal and cuspidal cubics

```
-- define the ring P
P = QQ[x,y]/(y^2+x^3+x^2)
-- define its normalization R
R = QQ[X,Y]/(Y^2+X+1)
-- the blow-up at the origin
-- defines an embedding P --> R
f = map(R, P, {X, X*Y})
-- define the principal ideal J
J = ideal(Y)
-- take I to be the contraction of J
I = preimage(f, J)
-- verify that I^2 is the contraction of J^2
I^2 == preimage(f, J^2)
-- verify that I^2 is principal
I^2 == ideal(x+1)
```

Figure 3.2. Macaulay-2 code verifying the assertions of Remark 3.27

4

Splitting the Knebusch-Milnor exact sequence

This chapter summarizes the results from [26, 28]. Here we further investigate the exact sequence of Theorem 1.57. Hence, as in Section 1.4 of the first chapter, $\Bbbk$ is a fixed real closed field, K is a formally real algebraic function field of one variable over $\Bbbk$ and γ is the associated real curve. We keep all the notation introduced in that section in particular $\gamma_1, \dots, \gamma_N$ are the semi-algebraically connected components of γ and R is the ring of regular functions on γ. By means of Theorem 1.57, from now on, we shall identify the Witt ring WR of the ring R of regular functions with its image under the canonical injection $W(R \rightarrowtail K)$. The main theorem of this chapter assert that the Knebusch-Milnor exact sequence splits (see Theorem 4.17). In particular the Witt group WR is a direct summand of the group WK (see Theorem 4.3). Moreover, if γ is affine and semi-algebraically connected, then the Witt group WP of the ring of polynomial functions is in turn a direct summand of WR (see Theorem 4.19). This means that the chain of rings $P \subset R \subset K$ gives rise to the associated chain of Witt groups $WP \subset WR \subset WK$ in which each element is a direct summand of its successor.

4.1. Preparatory lemmas

Recall that in Section 1.4 we defined $\lambda : \bigoplus WK(\mathfrak{p}) \cong \mathbb{Z}^{(\gamma)} \to \mathbb{Z}^N$ to be

$$\lambda\big((n_\mathfrak{p})_{\mathfrak{p}\in\gamma}\big) := \Big(\textstyle\sum_{\mathfrak{p}\in\gamma_1} n_\mathfrak{p}, \dots, \sum_{\mathfrak{p}\in\gamma_N} n_\mathfrak{p}\Big).$$

Let $H < \mathbb{Z}^{(\gamma)} \cong \bigoplus_{\mathfrak{p}\in\gamma} WK(\mathfrak{p})$ be the kernel of λ, i.e.

$$H = \Big\{(n_\mathfrak{p})_{\mathfrak{p}\in\gamma} \in \mathbb{Z}^{(\gamma)} : \sum_{\mathfrak{p}\in\gamma_i} n_\mathfrak{p} = 0 \text{ for all } 1 \le i \le N\Big\}. \tag{4.1}$$

Theorem 1.57 asserts that $H = \operatorname{im}\partial$. Select now a single point $\mathfrak{p}_i$ in each component γ_i of γ. The points $\mathfrak{p}_1 \in \gamma_1, \dots, \mathfrak{p}_N \in \gamma_N$ will remain fixed throughout the rest of this chapter. Denote $\mathscr{P} := \{\mathfrak{p}_1, \dots, \mathfrak{p}_N\}$ the set of these points. Further, let $\hat{H} < \mathbb{Z}^{(\gamma)}$ be the subgroup

$$\hat{H} = \big\{(n_\mathfrak{p})_{\mathfrak{p}\in\gamma} \in \mathbb{Z}^{(\gamma)} : n_\mathfrak{p} = 0 \text{ for } \mathfrak{p} \notin \mathscr{P}\big\}. \tag{4.2}$$

Proposition 4.1. *With the above notation, the group* $\mathbb{Z}^{(\gamma)}$ *is the direct sum of its subgroups* H *and* $\hat{H}$ *i.e.* $H \oplus \hat{H} = \mathbb{Z}^{(\gamma)}$.

Proof. Take an element $(n_{\mathfrak{p}})_{\mathfrak{p}\in\gamma} \in H \cap \hat{H}$. For every $1 \le i \le N$ we have

$$0 = \sum_{\mathfrak{p}\in\gamma_i} n_{\mathfrak{p}} = n_{\mathfrak{p}_i},$$

here the first equality is due to (4.1), while the latter one follows from (4.2). Hence $(n_{\mathfrak{p}})_{\mathfrak{p}\in\gamma} = 0$ and so $H \cap \hat{H} = \{0\}$.

Now, we show that $\mathbb{Z}^{(\gamma)} = H + \hat{H}$. Take an element $(n_{\mathfrak{p}})_{\mathfrak{p}\in\gamma} \in \mathbb{Z}^{(\gamma)}$ and let $m_i := \sum_{\mathfrak{p}\in\gamma_i} n_{\mathfrak{p}}$. We define two elements $\hat{h} \in \hat{H}$ and $h \in H$. The former being given by the condition

$$\hat{h} := (m_{\mathfrak{p}})_{\mathfrak{p}\in\gamma} \in \hat{H}, \qquad m_{\mathfrak{p}} = \begin{cases} m_i, & \text{for } \mathfrak{p} = \mathfrak{p}_i \\ 0, & \text{for } \mathfrak{p} \notin \{\mathfrak{p}_1, \dots, \mathfrak{p}_N\} \end{cases}$$

while the latter is given by

$$h := (s_{\mathfrak{p}})_{\mathfrak{p}\in\gamma}, \qquad s_{\mathfrak{p}} = \begin{cases} n_{\mathfrak{p}} - m_i, & \text{for } \mathfrak{p} = \mathfrak{p}_i \\ n_{\mathfrak{p}}, & \text{for } \mathfrak{p} \notin \{\mathfrak{p}_1, \dots, \mathfrak{p}_N\}. \end{cases}$$

Observe that $\sum_{\mathfrak{p}\in\gamma_i} s_{\mathfrak{p}} = \left(\sum_{\mathfrak{p}\in\gamma_i} n_{\mathfrak{p}}\right) - m_i = 0$, hence indeed $h \in H$. Clearly $h + \hat{h} = (n_{\mathfrak{p}})_{\mathfrak{p}\in\gamma}$. Consequently $\mathbb{Z}^{(\gamma)} = H \oplus \hat{H}$. ☐

We have a natural injection $l\colon \mathbb{Z}^N \to \mathbb{Z}^{(\gamma)}$ defined by the formula

$$l(n_1, \dots, n_N) := (n_{\mathfrak{p}})_{\mathfrak{p}\in\gamma} \quad \text{where } n_{\mathfrak{p}} = \begin{cases} n_i, & \text{for } \mathfrak{p} = \mathfrak{p}_i \\ 0, & \text{for } \mathfrak{p} \notin \mathscr{P}. \end{cases}$$

The following observation is immediate.

Observation 4.2. $\hat{H} = \operatorname{im} l$ *and* $\lambda \circ l = \mathrm{id}_{\mathbb{Z}^N}$.

Recall that for every two distinct points $\mathfrak{p}, \mathfrak{q}$ belonging to the same component γ_i there exists an interval function $\chi_{(\mathfrak{p},\mathfrak{q})}$, i.e. an element of K such that $\chi_{(\mathfrak{p},\mathfrak{q})}$ changes sign precisely at $\mathfrak{p}$, $\mathfrak{q}$ and is positive definite everywhere outside of the interval $(\mathfrak{p}, \mathfrak{q})$. An interval function is unique only up to multiplication by a totally positive element. Hence, in the following construction (as well as in the rest of this chapter), for every $\mathfrak{p} \in \gamma_i \setminus \{\mathfrak{p}_i\}$, we assume that $\chi_{(\mathfrak{p}_i,\mathfrak{p})}$ is an arbitrarily chosen and fixed interval function associated with the pair $(\mathfrak{p}_i, \mathfrak{p})$. Later, in Corollary 4.7, we show that this choice is not essential.

4.2. Direct sum theorem

For any $\mathfrak{q} \in \gamma$, let $\delta_{\mathfrak{q}}$ denote "Kronecker's delta", that is $\delta_{\mathfrak{q}} = (n_{\mathfrak{p}})_{\mathfrak{p}\in\gamma}$ with $n_{\mathfrak{p}} = 0$ for $\mathfrak{p} \neq \mathfrak{q}$ and $n_{\mathfrak{q}} = 1$. The set $\{\delta_{\mathfrak{q}} : \mathfrak{q} \in \gamma\}$ is a basis of the free $\mathbb{Z}$-module $\mathbb{Z}^{(\gamma)} \cong \bigoplus_{\mathfrak{p}\in\gamma} WK(\mathfrak{p})$. We define a group homomorphism $d\colon \bigoplus_{\mathfrak{p}\in\gamma} WK(\mathfrak{p}) \to WK$ by fixing its values on these generators as follows:

$$d(\delta_{\mathfrak{p}}) := \begin{cases} \langle \chi_{(\mathfrak{p}_i,\mathfrak{p})}\rangle, & \text{for } \mathfrak{p} \in \gamma_i \setminus \{\mathfrak{p}_i\} \\ 0, & \text{for } \mathfrak{p} \in \mathscr{P}. \end{cases} \tag{4.3}$$

Denote the image of this homomorphism by $D := \operatorname{im} d$. We are now ready to state the first main result of this chapter.

Theorem 4.3 (Direct sum theorem). *The Witt group WK of the formally real algebraic function field K over the real closed field $\Bbbk$ is a direct sum of the Witt ring WR of the ring R of regular functions on γ and the group D.*

The proof of this theorem occupies the rest of this section. However, before we proceed with a strict mathematical proof, let us first explain the main idea and highlight its milestones. The Witt ring of a field is additively generated by classes of one-dimensional forms. Thus, we shall prove that the class of every unary form $\langle f\rangle$ belongs to the sum $WR+D$. This is accomplished below by a sort of "induction on the degree of complexity" of f. First step is to prove the result for f totally positive; then for f being a single interval function (see Corollary 4.10); next, when f is a product of interval functions for intervals scattered among distinct components (see Lemma 4.11). Then, finally, we can take f to be an arbitrary function on γ. The main tool used in this "induction" is Corollary 4.6 below, providing a certain multiplication rule.

Lemma 4.4. *Let $f, g \in \dot K/\dot K^2$ be two square classes of K. If a binary form $\langle f, g\rangle$ represents 1 over K and both forms $\langle f\rangle$, $\langle g\rangle$ belong to the sum $WR + D$, then so does $\langle fg\rangle$.*

Proof. Suppose the form $\langle f, g\rangle$ represents 1, hence the forms $\langle f, g\rangle$ and $\langle 1, fg\rangle$ are isometric. Therefore, in the Witt ring WK we have:

$$\langle fg\rangle = \langle f\rangle + \langle g\rangle + \langle -1\rangle \in (WR + D) + (WR + D) + WR = WR + D. \qquad \square$$

For a given point $\mathfrak{p} \in \gamma$, let $\theta_{\mathfrak{p}}\colon \dot K/\dot K^2 \to \dot K_{\mathfrak{p}}/\dot K_{\mathfrak{p}}^2$ denote the group homomorphism induced by the canonical injection $K \rightarrowtail K_{\mathfrak{p}}$ of K into its completion $K_{\mathfrak{p}}$.

Lemma 4.5. *Let $f, g \in \dot K/\dot K^2$ be two square classes of K such that for almost every point $\mathfrak{p} \in \gamma$ either $\theta_{\mathfrak{p}} f$ or $\theta_{\mathfrak{p}} g$ is the unit element of $\dot K_{\mathfrak{p}}/\dot K_{\mathfrak{p}}^2$. Then the binary form $\langle f, g\rangle$ represents 1 over K.*

Proof. This follows immediately from Witt theorem (c.f. Theorem 1.55). $\square$

As simple as the above two lemmas are, they have some consequences. Recall, that for a given point $\mathfrak{p} \in \gamma$ and a quadratic form $\xi = \langle f_1, \dots, f_n \rangle$ over K we denote $\operatorname{sgn}_{\mathfrak{p}} \xi := \operatorname{sgn} f_1(\mathfrak{p}) + \dots + \operatorname{sgn} f_n(\mathfrak{p})$ the sign of ξ at $\mathfrak{p}$.

Corollary 4.6. *Let $f, g \in \dot K/\dot K^2$ be two square classes of K such that for almost every point $\mathfrak{p} \in \gamma$ either $\operatorname{sgn}_{\mathfrak{p}} f = 1$ or $\operatorname{sgn}_{\mathfrak{p}} g = 1$. If $\langle f\rangle, \langle g\rangle \in WR + D$, then also $\langle fg\rangle \in WR + D$.*

Observe that the above corollary implies that the square class of every totally positive element belongs to WR. Thus, we have:

Corollary 4.7. *Let $f, g \in \dot K/\dot K^2$ be two square classes of K such that the form $\langle f\rangle$ belongs to $WR + D$ and g is totally positive. Then $\langle fg\rangle \in WR + D$.*

Corollary 4.8. *Let $f, g \in \dot K/\dot K^2$ be two square classes of K such that for every point $\mathfrak{p} \in \gamma$ one has $\operatorname{sgn}_{\mathfrak{p}} f = \operatorname{sgn}_{\mathfrak{p}} g$. Then*

$$\langle f\rangle \in WR + D \iff \langle g\rangle \in WR + D.$$

Recall that in Section 1.3 we defined a subgroup $\mathbb{E} = \mathbb{E}(R)$ of the square class group $\dot K/\dot K^2$ of K by the formula

$$\mathbb{E} := \bigl\{ f \in \dot K/\dot K^2 : \operatorname{ord}_{\mathfrak{p}} f \equiv 0 \pmod 2 \text{ for every } \mathfrak{p} \in \gamma \bigr\}.$$

Lemma 4.9. *Let $f, g \in \dot K/\dot K^2$ be two square classes of K such that $f \in \mathbb{E}$ and $\langle g\rangle \in WR + D$. Then $\langle fg\rangle \in WR + D$.*

Proof. The Witt class of the form $\langle g\rangle$ may be expressed as $\langle g\rangle = \xi + \zeta$ for some $\xi \in WR$ and $\zeta \in D$. Therefore, in the Witt ring WK one has:

$$\langle fg\rangle = \langle f\rangle(\xi + \zeta) = \langle f\rangle \cdot \xi + \langle f\rangle \cdot \zeta.$$

The Witt ring WR of R is a subring of WK (recall that we identify here WR with its image under the canonical injection $W(R \rightarrowtail K)$) and so Corollary 1.46 implies that $\langle f\rangle \cdot \xi \in WR \subset WR + D$. Hence, all we need to show is that also $\langle f\rangle \cdot \zeta \in WR + D$.

Recall that $\mathbb{Z}^{(\gamma)}$ is generated by the set $\{\delta_{\mathfrak{p}} : \mathfrak{p} \in \gamma\}$. Consequently, $D = d(\mathbb{Z}^{(\gamma)})$ is spanned by $d\delta_{\mathfrak{p}}$ for $\mathfrak{p} \in \gamma$. In addition, $d\delta_{\mathfrak{p}_i} = 0$ for all $1 \le i \le N$ hence D is spanned by $\{d\delta_{\mathfrak{p}} : \mathfrak{p} \in \gamma \setminus \mathscr{P}\}$. Thus, all we need to show is that $\langle f\rangle \cdot d\delta_{\mathfrak{p}} = \langle f \cdot \chi_{(\mathfrak{p}_i, \mathfrak{p})}\rangle \in WR + D$ for every $\mathfrak{p} \in \gamma \setminus \mathscr{P}$. Fix a point $\mathfrak{p} \in \gamma$ and let $1 \le i \le N$ be the index of the component γ_i of γ containing $\mathfrak{p}$. Since $f \in \mathbb{E}$, so we see that $\operatorname{sgn}_* f$ does not vanish anywhere on γ. Consequently it is constant on every component of γ. Consider two cases. First, suppose that f is positive definite on γ_i (i.e. $\operatorname{sgn}|_{\gamma_i}(f) \equiv 1$). Take any point $\mathfrak{q} \in \gamma$. If $\mathfrak{q} \in \gamma_i$, then $\operatorname{sgn}_{\mathfrak{q}} f = 1$; otherwise if $\mathfrak{q} \in \gamma \setminus \gamma_i$, then $\operatorname{sgn}_{\mathfrak{q}} \chi_{(\mathfrak{p}_i, \mathfrak{p})} = 1$. Hence, Corollary 4.6 shows that $\langle f \cdot \chi_{(\mathfrak{p}_i, \mathfrak{p})}\rangle \in WR + D$. Now consider the second case, when f is negative definite on γ_i. Then $(-f)$ is positive definite on γ_i and the former case implies that $\langle -f \cdot \chi_{(\mathfrak{p}_i, \mathfrak{p})}\rangle \in WR + D$. Consequently also $\langle f \cdot \chi_{(\mathfrak{p}_i, \mathfrak{p})}\rangle \in WR + D$. □

Take $\mathfrak{p} \in \gamma_i$. By the very definition of d, the Witt class $\langle \chi_{(\mathfrak{p}_i,\mathfrak{p})} \rangle$ of the interval function $\chi_{(\mathfrak{p}_i,\mathfrak{p})}$ of the pair $(\mathfrak{p}_i, \mathfrak{p})$ belongs to $D \subset WR + D$. Hence, Corollary 4.8 implies that the Witt class of any interval function associated with the pair $(\mathfrak{p}_i, \mathfrak{p})$ belongs to $WR + D$. Now, let $\chi_{(\mathfrak{p},\mathfrak{p}_i)}$ be an interval function associated with the pair $(\mathfrak{p}, \mathfrak{p}_i)$. There exists a function f separating γ_i (see Theorem 1.52). In other words, there is $f \in \dot{K}/\dot{K}^2$ such that f is negative definite on γ_i and positive definite on $\gamma \setminus \gamma_i$. Clearly, $f \in \mathbb{E}(R)$ and so in the group $\dot{K}/\dot{K}^2$ we can write

$$\chi_{(\mathfrak{p},\mathfrak{p}_i)} = \chi_{(\mathfrak{p}_i,\mathfrak{p})} \cdot f \cdot g$$

for some totally positive g. The previous lemma, together with Corollary 4.7 imply that the form $\langle \chi_{(\mathfrak{p},\mathfrak{p}_i)} \rangle$ belongs to $WR + D$. Thus we have just proved:

Corollary 4.10. *For every component γ_i and every point $\mathfrak{p} \in \gamma_i$ the Witt class of the form $\langle \chi_{(\mathfrak{p},\mathfrak{p}_i)} \rangle$ of an interval function of the pair $(\mathfrak{p}, \mathfrak{p}_i)$ belongs to $WR + D$.*

So far we have dealt with just single intervals. Now we turn our attention to the case when we have a few intervals, each in a different component.

Lemma 4.11. *Let $\emptyset \neq I \subseteq \{1, \dots, N\}$ be some non-empty set of indices. For every $i \in I$ let $\mathfrak{q}_i \in \gamma_i \setminus \{\mathfrak{p}_i\}$ be a fixed point and let g_i denote the square class of either $\chi_{(\mathfrak{q}_i,\mathfrak{p}_i)}$ or $\chi_{(\mathfrak{p}_i,\mathfrak{q}_i)}$. Then the unary form $\langle g \rangle$ of the square class $g := \prod_{i \in I} g_i$ belongs to $WR + D$.*

Proof. We proceed by induction on the number of elements in I. The previous corollary proves the initial case when $\operatorname{card} I = 1$. Assume that we have proved the assertion for all $n < \operatorname{card} I$ and let $k := \min I$. Factor g into $g = g_k \cdot \hat{g}$ with $\hat{g} = g/g_k$ being the product of all g_i except g_k. Now, both g_k and $\hat{g}$ belong to $WR + D$ by the induction, hence Corollary 4.6 implies that also $\langle g \rangle \in WR + D$. □

Recall that for every point $\mathfrak{p} \in \gamma$ there are exactly two orderings $\beta_+(\mathfrak{p})$ and $\beta_-(\mathfrak{p})$ of the field K compatible with $\mathfrak{p}$.

Lemma 4.12. *Let $f \in \dot{K}/\dot{K}^2$ be a square class of K, then $\langle f \rangle \in WR + D$.*

Proof. We proceed by induction on $s = \operatorname{card}\{\mathfrak{p} \in \gamma : \operatorname{sgn}_{\mathfrak{p}} f = 0\}$. As we know (see Theorem 1.53) the number s is even. If $s = 0$, then $f \in \mathbb{E}(R)$ and so Corollary 1.46 implies that $\langle f \rangle \in WR \subset WR + D$. Assume that we have proved the result for all even integers less than s.

By means of Theorem 1.52 we can find square classes $e_1, \dots, e_N \in \mathbb{E}(R)$ separating components $\gamma_1, \dots, \gamma_N$, this means that e_i is positive definite on $\gamma \setminus \gamma_i$ and negative definite on γ_i. Take $J \subseteq \{1, \dots, N\}$ to be the set of all those indices $1 \leq i \leq N$ such that f is negative with respect to $\beta_-(\mathfrak{p}_i)$. In other words

$$J := \{1 \leq i \leq N : f \notin \beta_-(\mathfrak{p}_i)\}.$$

Take $f' := f \cdot \prod_{i\in J} e_i$. Lemma 4.9 implies that $\langle f\rangle \in WR + D$ if and only if $\langle f'\rangle \in WR + D$. On the other hand, one has

$$\operatorname{sgn}_{\mathfrak{p}} f = 0 \iff \operatorname{sgn}_{\mathfrak{p}} f' = 0.$$

Moreover f' is positive with respect to every $\beta_-(\mathfrak{p}_i)$ for $1 \le i \le N$. Therefore, for the rest of this proof, we can substitute f by f'. Thus, from now on, we assume that $f \in \beta_-(\mathfrak{p}_i)$ for all $1 \le i \le N$.

A priori, it is possible that f changes sign at some $\mathfrak{p}_i \in \mathscr{P}$. Let I be the set of all such i's, i.e. $I := \{1 \le i \le N : \operatorname{sgn}_{\mathfrak{p}_i} f = 0\}$. For every $i \in I$ let $\mathfrak{q}_i \in \gamma_i \setminus \{\mathfrak{p}_i\}$ be a point such that $\operatorname{sgn}_{\mathfrak{q}_i} f = 0$ and $\operatorname{sgn}_{\mathfrak{r}} f \neq 0$ for all $\mathfrak{r} \in (\mathfrak{p}_i, \mathfrak{q}_i)$ (in a common language: $\mathfrak{q}_i$ is the first zero of $\operatorname{sgn}_* f$ right to $\mathfrak{p}_i$). Let f_i be either $\chi_{(\mathfrak{p}_i,\mathfrak{q}_i)}$ if $i \in I$ or $f_i := 1$ if $i \notin I$ $(1 \le i \le N)$. Again, $\chi_{(\mathfrak{p}_i,\mathfrak{q}_i)}$ is an interval function for the pair $(\mathfrak{p}_i, \mathfrak{q}_i)$. Take $\hat{f}, \tilde{f} \in \dot{K}/\dot{K}^2$ given by $\hat{f} := f_1 \cdots f_N$ and $\tilde{f} := f \cdot \hat{f}$. Obviously $\operatorname{sgn}_{\mathfrak{p}_i} \tilde{f} = 1$ for all $1 \le i \le N$. Moreover

$$\bigl\{\mathfrak{p} \in \gamma : \operatorname{sgn}_{\mathfrak{p}} \tilde{f} = 0\bigr\} = \bigl\{\mathfrak{p} \in \gamma : \operatorname{sgn}_{\mathfrak{p}} f = 0\bigr\} \setminus \bigcup_{i\in I}\{\mathfrak{p}_i, \mathfrak{q}_i\}.$$

Thus, if I is not empty, then $\langle \tilde{f}\rangle \in WR + D$ by the induction hypothesis. Lemma 4.11 asserts that also $\langle \hat{f}\rangle \in WR + D$. Finally, for a given point $\mathfrak{p} \in \gamma$ either $\mathfrak{p} \in \bigcup_{i\in I}(\mathfrak{p}_i, \mathfrak{q}_i)$, then $\operatorname{sgn}_{\mathfrak{p}} \tilde{f} = 1$ or $\mathfrak{p} \notin \bigcup_{i\in I}[\mathfrak{p}_i, \mathfrak{q}_i]$, and then $\operatorname{sgn}_{\mathfrak{p}} \hat{f} = 1$. All in all, Corollary 4.6 shows that $\langle f\rangle \in WR + D$.

Therefore, assume now that I is empty, this means that $\operatorname{sgn}_{\mathfrak{p}_i} f = 1$ for all $1 \le i \le N$. Let

$$\mathfrak{q}^1_1, \ldots, \mathfrak{q}^1_{s_1}, \mathfrak{q}^2_1, \ldots, \mathfrak{q}^2_{s_2}, \ldots, \mathfrak{q}^N_1, \ldots, \mathfrak{q}^N_{s_N}$$

be all the points of γ where $\operatorname{sgn}_* f$ vanishes. We assume here that $\mathfrak{q}^i_j \in \gamma_i$ and so $s_1 + \cdots + s_N = s$, $s_i \in 2\mathbb{Z}$, $s_i \ge 0$. For every $1 \le i \le N$ we renumber points $\mathfrak{q}^i_j$ $(1 \le j \le s_i)$ in such a way (see Figure 4.1), that the consecutive intervals form an ascending chain:

$$\mathfrak{p}_i \in (\mathfrak{q}^i_1, \mathfrak{q}^i_2) \subsetneq (\mathfrak{q}^i_3, \mathfrak{q}^i_4) \subsetneq \cdots \subsetneq (\mathfrak{q}^i_{s_i-1}, \mathfrak{q}^i_{s_i}).$$

Since $\operatorname{sgn}_{\mathfrak{p}_i} f = 1$, so we have

$$\partial_{\mathfrak{q}^i_1} f = 1, \partial_{\mathfrak{q}^i_2} f = -1, \partial_{\mathfrak{q}^i_3} f = -1, \ldots, \partial_{\mathfrak{q}^i_j} f = (-1)^{\lfloor \frac{j}{2} \rfloor}, \ldots$$

for every $1 \le i \le N$ and $1 \le j \le s_i$. Let χ^i_j be the interval function for either $(\mathfrak{q}^i_j, \mathfrak{p}_i)$ if $j \notin 2\mathbb{Z}$ or $(\mathfrak{p}_i, \mathfrak{q}^i_j)$ if $j \in 2\mathbb{Z}$. Define square classes g_i, h_i for $1 \le i \le N$ by the formulas:

$$g_i := \begin{cases} \prod\limits_{\substack{1\le j\le s_i-1\\ j\notin 2\mathbb{Z}}} \chi^i_j & \text{for } s_i \neq 0\\ 1 & \text{for } s_i = 0\end{cases} \qquad h_i := \begin{cases} \prod\limits_{\substack{2\le j\le s_i\\ j\in 2\mathbb{Z}}} \chi^i_j & \text{for } s_i \neq 0\\ 1 & \text{for } s_i = 0.\end{cases}$$

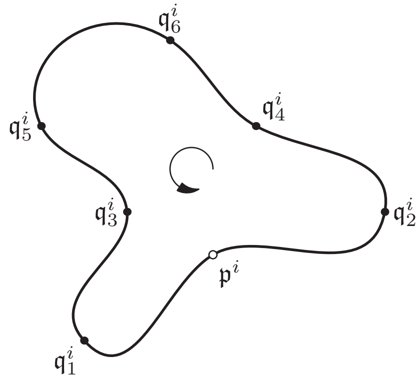


Figure 4.1. Numbering of $\mathfrak{q}_j^i$ on γ_i

Take $g := g_1 \cdots g_N$ and $h := h_1 \cdots h_N$. There is a totally positive $e \in \dot{K}/\dot{K}^2$ such that equality $f = g \cdot h \cdot e$ holds in the square class group $\dot{K}/\dot{K}^2$. By means of Corollary 4.7 it is enough to show that $\langle g \cdot h \rangle \in WR + D$.

If $s_i \leq 2$ for all $1 \leq i \leq N$, then Lemma 4.11 implies that $\langle g \rangle, \langle h \rangle \in WR + D$. Otherwise, if $s_i > 2$ for some i, then

$$\begin{aligned}\operatorname{card}\bigl\{\mathfrak{p} \in \gamma : \operatorname{sgn}_{\mathfrak{p}} g = 0\bigr\} = \operatorname{card}\bigl\{\mathfrak{p} \in \gamma : \operatorname{sgn}_{\mathfrak{p}} h = 0\bigr\} = \\ = \sum_{1 \leq i \leq N} 2 \cdot \left\lceil \frac{s_i}{4} \right\rceil < \sum_{1 \leq i \leq N} s_i = s,\end{aligned}$$

and so $\langle g \rangle, \langle h \rangle \in WR + D$ by our inductive hypothesis. As we see, in both cases the forms $\langle g \rangle, \langle h \rangle$ belong to $WR + D$, hence Corollary 4.6 asserts that $\langle g \cdot h \rangle \in WR + D$, as well. □

The Witt group WK of the field K is generated by classes of forms of dimension one. Hence, we conclude:

Corollary 4.13. *$WK = WR + D$.*

In order to complete the proof of Theorem 4.3 we need show that $WR \cap D = \{0\}$. To accomplish this we prove the following lemma.

Lemma 4.14. *The composition $(\partial \circ d)|_H$ is the identity on H.*

Proof. Notice that H is spanned by sequences of the form $\delta_{\mathfrak{p}} - \delta_{\mathfrak{p}_i}$ for $\mathfrak{p} \in \gamma_i \setminus \{\mathfrak{p}_i\}$ and $1 \leq i \leq N$. Hence, we restrict ourselves to such elements. Now, however, we have

$$\delta_{\mathfrak{p}} - \delta_{\mathfrak{p}_i} \xmapsto{d} \langle \chi_{(\mathfrak{p}_i, \mathfrak{p})} \rangle \xmapsto{\partial} \delta_{\mathfrak{p}} - \delta_{\mathfrak{p}_i}.$$ □

Recall that the group $\hat{H}$ was defined in Eq. (4.2).

Corollary 4.15. *The kernel* $\ker d$ *of* d *equals* $\hat{H}$.

Proof. The inclusion $\hat{H} \subseteq \ker d$ is trivial. We show the other one. Take any $\xi \in \ker d$. Proposition 4.1 states that $\bigoplus_{\mathfrak{p}\in\gamma} WK(\mathfrak{p}) = H \oplus \hat{H}$, so we can (uniquely) express ξ as a sum $\xi = h + \hat{h}$, with $h \in H$ and $\hat{h} \in \hat{H}$. Since $\hat{H} \subseteq \ker d$, we have $d\xi = dh + d\hat{h} = dh$. The previous lemma implies that $(\partial \circ d)(h) = h$. Now, ξ was taken from the kernel of d, thus

$$0 = \partial(0) = (\partial \circ d)(\xi) = (\partial \circ d)(h) = h.$$

All in all, $\xi = \hat{h} \in \hat{H}$ and so $\ker d = \hat{H}$, as desired. $\square$

We are now ready to conclude the proof of Theorem 4.3.

Corollary 4.16. $WR \cap D = \{0\}$.

Proof. Take any $\zeta \in WR \cap D$. Since $\zeta \in D$, hence there is $\xi \in \bigoplus_{\mathfrak{p}\in\gamma} WK(\mathfrak{p})$ such that $\zeta = d\xi$. By means of the above corollary we may assume that $\xi \in H$. Now, Lemma 4.14 implies that $\xi = (\partial \circ d)(\xi) = \partial\zeta$. But $WR = \ker \partial$ (see Theorem 1.57) and so $\xi = 0$. Thus also $\zeta = d\xi = 0$. $\square$

Now, Theorem 4.3 follows immediately from Corollaries 4.13 and 4.16.

4.3. Splitting theorem

The notion of splitting exact sequences is normally defined for sequences having only three non-zero terms. Anyway, the above result shows that the Knebusch-Milnor exact sequence for the Witt group of a ring of regular functions admits a full analogy of splitting. To state it precisely, we formulate the main result of this chapter. Let $\pi\colon WK = WR \oplus D \to WR$ be the projection of WK onto WR.

Theorem 4.17. *The following two sequences are exact*

$$0 \rightleftarrows WR \underset{\pi}{\overset{i}{\rightleftarrows}} WK \underset{d}{\overset{\partial}{\rightleftarrows}} \bigoplus_{\mathfrak{p}\in\gamma} WK(\mathfrak{p}) \underset{l}{\overset{\lambda}{\rightleftarrows}} \mathbb{Z}^N \rightleftarrows 0.$$

Moreover:

1. $WK = \operatorname{im} i \oplus \operatorname{im} d = \ker \partial \oplus \ker \pi$;
2. $\bigoplus_{\mathfrak{p}\in\gamma} WK(\mathfrak{p}) = \operatorname{im} \partial \oplus \operatorname{im} l = \ker \lambda \oplus \ker d$;
3. $\lambda \circ l = \mathrm{id}_{\mathbb{Z}^N}$;
4. $\pi \circ i = \mathrm{id}_{WR}$;
5. $(\partial \circ d)|_H = \mathrm{id}_H$;
6. $(d \circ \partial)|_D = \mathrm{id}_D$.

Proof. The upper sequence is just the Knebusch-Milnor exact sequence (c.f. Theorem 1.57). The exactness of the lower sequence at $\bigoplus_{\mathfrak{p}\in\gamma} WK(\mathfrak{p})$ follows from Observation 4.2 together with Corollary 4.15. Next, Theorem 4.3 implies the exactness at WK. As to the "moreover" part: point (4.17) follows from Theorem 4.3; point (4.17) from Proposition 4.1; point (4.17) from Observation 4.2; (4.17) is trivial; (4.17) was proved in Lemma 4.14. All in all, we only need to show (4.17). Take $\zeta \in D$, there is $\xi \in H$ such that $d\xi = \zeta$. Hence, $\partial\zeta = (\partial \circ d)(\xi) = \xi$ and so $(d \circ \partial)(\zeta) = d\xi = \zeta$. □

We can rephrase the above result, with a more homological flavor, using the language of slicing and patching, as follows:

Corollary 4.18. *The exact sequence*

$$0 \to WR \xrightarrow{i} WK \xrightarrow{\partial} \bigoplus_{\mathfrak{p}\in\gamma} WK(\mathfrak{p}) \xrightarrow{\lambda} \mathbb{Z}^N \to 0.$$

slices into and is patched by the following two split exact sequences:

$$0 \to WR \to WK \to H \to 0 \qquad \textit{and} \qquad 0 \to D \to \bigoplus_{\mathfrak{p}\in\gamma} WK(\mathfrak{p}) \to \mathbb{Z}^N \to 0.$$

4.4. Further splitting

So far in this chapter, we implicitly treated $\Omega(K)$ as a subset of the projective plane $\mathbb{P}^2\Bbbk(\sqrt{-1})$ without any reference to the notion of affinity/infinity. However, if we fix an affine plane $\mathbb{A}^2\Bbbk(\sqrt{-1}) \subset \mathbb{P}^2\Bbbk(\sqrt{-1})$, we may consider the affine curve $C := \Omega(K) \cap \mathbb{A}^2\Bbbk(\sqrt{-1})$ and respectively the affine real curve $\gamma_a := C \cap \mathbb{A}^2\Bbbk$. This leads to the notion of the *ring of polynomial functions* on C:

$$P := \bigcap_{\mathfrak{p}\in C} \mathcal{O}_{\mathfrak{p}},$$

here as always, $\mathcal{O}_{\mathfrak{p}}$ denotes the valuation subring of K associated with the point $\mathfrak{p}$. The ring P is again a Dedekind domain, hence $W(P \rightarrowtail K)$ is a monomorphism by Theorem 1.40. The rings: R of regular functions on γ and P of polynomial functions on C are, in general, distinct. Nevertheless, if the real affine part γ_a is semi-algebraically compact, then γ does not have any points at infinity, hence $\gamma = \gamma_a$. Consequently P is a subring of R. We can, thus, consider a map $W(P \rightarrowtail R)$. Obviously this is a monomorphism, as both are Dedekind domains. However, in the view of the previous sections, the natural question is whether this monomorphism splits, i.e. whether the image of WP is a direct summand of the Witt group WR. It turns out that the answer is affirmative providing that γ is semi-algebraically connected.

Theorem 4.19. *With the above notation, if γ is affine semi-algebraically compact and semi-algebraically connected, then the Witt group WP of the ring P of polynomial functions is a direct summand of the Witt group WR of the ring of regular functions. In particular, WP is a direct summand of WK, as well.*

The "in particular" part of the above result follows from the main part by means of Theorem 4.3, but, in fact, we will show it directly in the course of the proof. In the rest of this section we keep the assumptions of the theorem, without repeating in every lemma, over and over again. Note the following immediate consequence of the semi-algebraic connectedness of γ:

Observation 4.20. *Under the assumptions of Theorem 4.19 one has*

$$\mathbb{E}(R) = \pm \sum \dot{K}^2.$$

Let us first define a group S, which will turn out to be a direct-sum completion of WP in WR. The group $\mathbb{E}(P)$ is a subgroup of $\mathbb{E}(R)$ Now, since the rank of every element of $\mathbb{E}(R) \subset \dot{K}/\dot{K}^2$ equals 2, we may treat $\mathbb{E}(R)$ as a $\mathbb{F}_2$-linear space and $\mathbb{E}(P)$ as its subspace. Therefore $\mathbb{E}(P)$ is a direct summand of $\mathbb{E}(R)$, say, $\mathbb{E}(R) = \mathbb{E}(P) \oplus E'$ for some subspace E' which is again a subgroup of $\mathbb{E}(R)$. The square class of -1 belongs to $\mathbb{E}(P)$, hence, without loss of generality, we may assume that $E' \subset \sum \dot{K}^2$. Define S to be the subgroup of the Witt group WK generated by the set $\{\langle -1, f\rangle : f \in E'\}$.

Lemma 4.21. *The following hold*

1. *$S \subset WR$;*
2. *$2S \subset \{0\}$;*
3. *S contains no classes of unary forms.*

Proof. The first assertion follows immediately from Corollary 1.46. Further, (4.21) follows from (4.21). Therefore, it remains to prove (4.21). It suffices to show that every generator of S is of rank two. Take $f \in E' \subset \sum \dot{K}^2$. Now $\langle f, f\rangle = \langle 1, 1\rangle$, so that $\langle -1, f\rangle + \langle -1, f\rangle = 0$ in WK. Since WR embeds in WK, this sum is also null in WR. □

Lemma 4.22. *$WP \cap S = \{0\}$.*

Proof. Suppose, a contrario, that there is a non-hyperbolic form ξ over K, and its class belongs to the intersection $WP \cap S$. Now, ξ being an element of S, is of the form

$$\xi = \pm\langle -1, f_1\rangle \pm \cdots \pm \langle -1, f_n\rangle.$$

for some $f_1, ..., f_n \in E'$. By Lemma 4.21 (4.21), we may assume that $f_1, \ldots, f_n$ are pairwise distinct as elements of $\dot{K}/\dot{K}^2$. One easily checks that the discriminant of ξ equals $f_1 \cdots f_n$, and hence $\operatorname{disc} \xi \in E'$. On the other hand, by Corollary 1.47,

$\operatorname{disc}\xi \in \mathbb{E}(P)$. Therefore, $\operatorname{disc}\xi \in \mathbb{E}(P) \cap E' = \{1\}$. If $n = 1$, then $\xi = \langle -1, f_1 \rangle$. Consequently f is a square, hence ξ is the zero element of the Witt ring WP. Now, suppose that $n > 1$. It is clear that $\operatorname{sgn}_{\mathfrak{p}} \xi = 0$ for every $\mathfrak{p} \in \gamma$. It follows from Corollary 1.56 that again ξ is the null element of WP. □

From the above two lemmas it follows that $WP \oplus S$ is a subgroup of WR. We need to prove that it is equal to WR. Firstly, we shall show that it contains all the classes of forms of dimensions ≤ 2 over K that belong to WR (see Propositions 4.23 and 4.24).

PROPOSITION 4.23. *For every $f \in \mathbb{E}(R)$, $\langle f \rangle \in WP \oplus S$.*

Proof. Take $f \in \mathbb{E}(R) = \pm \sum \dot{K}^2$. Suppose that $f \in -\sum \dot{K}^2$. Since $\mathbb{E}(R) = \mathbb{E}(P) \oplus E'$, therefore there exist the unique $e \in \mathbb{E}(P)$ and $e' \in E'$ such that $e \cdot e' = f$. Now, $e' \in E' \subset \sum \dot{K}^2$, hence $e = f \cdot e' \in -\sum \dot{K}^2$. By the Witt theorem (see Theorem 1.55), the form $\langle e, e' \rangle$ represents 1 over K. Consequently, $\langle e, e' \rangle = \langle 1, ee' \rangle = \langle 1, f \rangle$, therefore

$$\langle f \rangle = \langle e \rangle + \langle -1, e' \rangle \in WP \oplus S.$$

Now assume that $f \in \sum \dot{K}^2$. By the previous part, $\langle -f \rangle$ belongs to $WP \oplus S$, and so does $\langle f \rangle$. □

PROPOSITION 4.24. *For every $f, g \in \dot{K}/\dot{K}^2$, if $\langle f, g \rangle \in WR$, then $\langle f, g \rangle \in WP \oplus S$.*

Proof. Let $\langle f, g \rangle \in WR$. Therefore, $fg \in \pm \sum \dot{K}^2$, by Corollary 1.47 and Observation 4.20. Firstly, suppose that $h := fg \in \sum \dot{K}^2$. We claim that f may not change sign at any point of γ. Indeed, if f changes sign at $\mathfrak{p}$, then $\partial_{\mathfrak{p}} \langle f, fh \rangle = \langle 1, 1 \rangle \neq 0$. Thus $\langle f, g \rangle = \langle f, fh \rangle \notin \ker \partial_R = WR$, which is a contradiction. Now, since γ is semi-algebraically connected, $f \in \pm \sum \dot{K}^2 = \mathbb{E}(R)$. Using Proposition 4.23 we show that $\langle f \rangle, \langle fh \rangle \in WP \oplus S$. Thus, also $\langle f, g \rangle = \langle f \rangle + \langle fh \rangle \in WP \oplus S$.

On the other hand, if $fg \in -\sum \dot{K}^2$, then $\operatorname{sgn}_{\mathfrak{p}} f = -\operatorname{sgn}_{\mathfrak{p}} g$ for every real point $\mathfrak{p}$. Hence, by the Witt theorem, the forms $\langle f, g \rangle$ and $\langle 1, fg \rangle$ are isometric. Thus $\langle 1, fg \rangle \in WR$, and so $\langle fg \rangle \in WR$. Now, Corollary 1.46 and Proposition 4.23 assert that $\langle fg \rangle \in WP \oplus S$ and consequently $\langle f, g \rangle = \langle 1 \rangle + \langle fg \rangle \in WP \oplus S$. □

Now, once we are done with unary and binary forms, we may turn our attention to forms of higher dimensions. Those, however, require a more general approach. Fix a real point $\mathfrak{p}_0 \in \gamma$. As in the previous sections, for every $\mathfrak{p} \in \gamma \setminus \{\mathfrak{p}_0\}$, let $\chi_{(\mathfrak{p}_0, \mathfrak{p})}$ be an arbitrary chosen and fixed interval function of $(\mathfrak{p}_0, \mathfrak{p})$. Assume further that the interval functions are chosen in such a way that $\chi_{(\mathfrak{p}, \mathfrak{p}_0)} := -\chi_{(\mathfrak{p}_0, \mathfrak{p})}$. Recall that D is the subgroup of WK generated by the set $\{\langle \chi_{(\mathfrak{p}_0, \mathfrak{p})} \rangle : \mathfrak{p} \neq \mathfrak{p}_0\}$. The group WK decomposes as $WK = WR \oplus D$. We know that $WP \oplus S \subseteq WR$, hence once we show that $WP \oplus S \oplus D = WK$, it will follow that $WR = WP \oplus S$.

Lemma 4.25. *Let $f, g \in \dot{K}/\dot{K}^2$ be two square classes of K such that, for almost every point $\mathfrak{p} \in \gamma$, either $f(\mathfrak{p}) > 0$ or $g(\mathfrak{p}) > 0$. If $\langle f\rangle, \langle g\rangle \in WP \oplus S \oplus D$, then also $\langle fg\rangle \in WP \oplus S \oplus D$.*

Proof. Forms $\langle f, g\rangle$ and $\langle 1, fg\rangle$ are isometric by the Witt theorem, hence $\langle fg\rangle = \langle f\rangle + \langle g\rangle + \langle -1\rangle \in WP \oplus S \oplus D$. □

Lemma 4.26. *Let $f \in \dot{K}/\dot{K}^2$ be a square class. Assume that f changes sign at exactly two points of γ. Then $\langle f\rangle \in WP \oplus S \oplus D$.*

Proof. Firstly, assume that f changes sign at $\mathfrak{p}_0$. Therefore, there exists a sum of squares $g \in \sum \dot{K}^2$ and a point $\mathfrak{p} \in \gamma \setminus \{\mathfrak{p}_0\}$ such that $f = \pm\chi_{(\mathfrak{p}_0,\mathfrak{p})} \cdot g$. Now, by the definition of D we have $\langle \chi_{(\mathfrak{p}_0,\mathfrak{p})}\rangle \in D \subset WP \oplus S \oplus D$. On the other hand $\langle g\rangle \in WP \oplus S \subset WP \oplus S \oplus D$ by Proposition 4.23. Consequently, the previous lemma asserts that $\langle f\rangle \in WP \oplus S \oplus D$.

Now assume that f does not change sign at $\mathfrak{p}_0$. Let $\mathfrak{p}, \mathfrak{q}$ be the two points where f changes sign. The curve γ is homeomorphic to a circle, hence, without loss of generality, we may assume that $\mathfrak{p}_0 \in (\mathfrak{p}, \mathfrak{q})$. We may once again write $f = \pm\chi_{(\mathfrak{p}_0,\mathfrak{p})} \cdot \chi_{((\mathfrak{p}_0,\mathfrak{q}))} \cdot g$ for a certain sum of squares g. We proceed as above to show that $\langle f\rangle \in WP \oplus S \oplus D$, only now we use Lemma 4.25 twice instead of just once. □

We are now ready to prove the theorem.

Proof of Theorem 4.19. Take any square class $f \in \dot{K}/\dot{K}^2$ of K. We will show that $\langle f\rangle \in WP \oplus S \oplus D$. Let s be half the number of sign changes of f on γ. Proceed by induction on s: if $s = 0$, then $f \in \pm\sum \dot{K}^2$, and so $\langle f\rangle \in WP \oplus S \subset WP \oplus S \oplus D$, by Proposition 4.23. If $s = 1$, then $\langle f\rangle \in WP \oplus S \oplus D$, by Lemma 4.26. Assume that we have proved the assertion for every integer less than s. Take $\mathfrak{p}, \mathfrak{q}$ to be two consecutive points where f changes sign (i.e. f changes sign at $\mathfrak{p}$ and $\mathfrak{q}$ but not in-between). Without loss of generality we may assume that $\operatorname{sgn}_{\mathfrak{r}} f = -1$ for $\mathfrak{r} \in (\mathfrak{p}, \mathfrak{q})$. Let $\tilde{f} := f \cdot \chi_{(\mathfrak{p},\mathfrak{q})}$. Then $\tilde{f}$ changes sign at $2s - 2$ points (i.e. in all the points where f does except $\mathfrak{p}$ and $\mathfrak{q}$), hence, by the inductive hypothesis, $\langle \tilde{f}\rangle \in WP \oplus S \oplus D$. Moreover, $\langle \chi_{(\mathfrak{p},\mathfrak{q})}\rangle \in WP \oplus S \oplus D$, by Lemma 4.26. Thus $\langle f\rangle = \langle \tilde{f} \cdot \chi_{(\mathfrak{p},\mathfrak{q})}\rangle \in WP \oplus S \oplus D$, by Lemma 4.25.

We have thus shown that, for every unary form over K, its class belongs to the direct sum $WP \oplus S \oplus D$. The Witt group of a field is generated by classes of unary forms, hence $WK = WP \oplus S \oplus D$. Now, since $WK = WR \oplus D$ (see Theorem 4.3) and $WP \oplus S \subseteq WR$, we have $WP \oplus S = WR$. □

5

Witt equivalence of real rings

The ultimate question in the algebraic theory of quadratic forms is whether the Witt rings WP and WR of two given rings P and R are isomorphic. If this is the case, we say that the rings P, R are *Witt equivalent*. This problem is difficult even over fields and has been investigated in numerous papers over the last 40 years. So far it has been solved only in a few cases. The three main are: fields having no more than 32 square classes (see [9]), global fields — this area has been most actively investigated in previous years (see e.g. [44, 52, 53]) and fields of rational functions on algebraic curves (see [23, 24, 25]). The pursuit for criteria of Witt equivalence of rings has started only recently (see e.g. [46, 47, 27, 29]).

The full treatise on all the above mentioned results would certainly exceed the limited scope of this chapter. Thus, we concentrate only on one particular case. Below we present a recent result of Grenier-Boley and Hoffmann (see Theorem 5.3) which generalizes an earlier result of the author (see Proposition 5.22 and Theorem 5.23). Theorem of Grenier-Boley and Hoffmann gives a criterion for Witt equivalence of two formally real fields providing that their u-invariants do not exceed two. Next, we concentrate on the real holomorphy subrings of such two fields. We show (see Theorem 5.15) that if the fields are *tamely* equivalent, then not only the fields, but also their holomorphy rings, are Witt equivalent. Moreover, the Witt isomorphism of the holomorphy rings is a restriction of the Witt isomorphism of fields. This result generalizes a result obtained earlier in [27].

5.1. Witt equivalence of real fields

The main tool to cope with Witt equivalence of any two arbitrary fields is the following *Harrison's criterion*:

Harrison Theorem 5.1. *Let K and L be fields of characteristic different from two. Then K, L are Witt equivalent if and only if there exists an isomorphism $t : \dot{K}/\dot{K}^2 \to \dot{L}/\dot{L}^2$ of their square-class groups taking -1 to -1 and such that a binary form $\langle a, b\rangle$ represents 1 over K if and only if $\langle ta, tb\rangle$ represents 1 over L.*

As for the proof, we refer the reader to [33, Theorem XII.1.8] The isomorphism t from the above theorem is called *Harrison's isomorphism*. If t is a Harrison's isomorphism, then the mapping $i_t : WK \to WL$ given by $i_t\langle a_1, \cdots, a_n\rangle := \langle ta_1, \cdots, ta_n\rangle$ is an isomorphism of Witt rings. We call it the *strong* isomorphism associated with the Harrison map t.

The space of ordering $\mathcal{X}_K$ and Harrison topology was introduced earlier in Section 1.2. Recall (see e.g. [33, Chapter XI]) that the (general) *u-invariant* $u(K)$ of an arbitrary field K is the maximum dimension of an anisotropic form ξ such that its Witt class is torsion. We take $u(K) := \infty$ if the maximum does not exist.

Definition 5.2. Two formally real fields K and L are said to be *$\mathcal{X}$-equivalent* if there exists a pair of maps (t, T) in which $T : \mathcal{X}_K \to \mathcal{X}_L$ is a homeomorphism of the spaces of orderings and $t : \dot{K}/\dot{K}^2 \to \dot{L}/\dot{L}^2$ is an isomorphism of the square-class groups preserving the signatures in the sense that

$$\forall_{\beta \in \mathcal{X}_K} \forall_{a \in K} a \in \beta \iff ta \in T\beta.$$

Theorem 5.3 ([19, Theorem 1.3]). *Let K, L be two formally real fields and assume that their u-invariants satisfy $\max\{u(K), u(L)\} \leq 2$. Then the following two conditions are equivalent:*

- *K, L are Witt equivalent;*
- *K, L are $\mathcal{X}$-equivalent.*

In order to prove the above theorem we need the following lemma. We keep the assumptions on K and L as in the theorem.

Lemma 5.4. *If K, L are $\mathcal{X}$-equivalent, then there is an $\mathcal{X}$-equivalence (t, T) in which $t(-1) = -1$.*

Proof. Let (t_1, T_1) be any $\mathcal{X}$-equivalence of K and L. Since -1 is totally negative, then so is $t_1(-1)$. By the Artin's Theorem, $-t_1(-1)$ is a sum of squares in L. Hence, either $-t_1(-1) = 1$ in which case we don't need to do anything, or the set $\{-1, -t_1(-1)\}$ may be extended to a basis $\mathscr{B}$ of the $\mathbb{F}_2$-vector space $\dot{L}/\dot{L}^2$ and let $\mathscr{A} := \mathscr{B} \setminus \{-1, -t_1(-1)\}$. Take the linear automorphism t^* of $\dot{L}/\dot{L}^2$ such that

$$t^*(-1) = -t_1(-1), \qquad t^*\big(-t_1(-1)\big) = -1, \qquad t^* \big|_{\mathscr{A}} = \mathrm{id}_{\mathscr{A}} .$$

Take now $t := t^* \circ t_1$ and $T := T_1$, then (t, T) is the desired $\mathcal{X}$-equivalence. Indeed, $a \in \beta$ if and only if $t_1(a) \in T_1\beta$ but this is equivalent to $t(a) \in T\beta$ since both -1 and $-t_1(-1)$ are totally negative. It is obvious that $t(-1) = -1$. □

Proof of Theorem 5.3. Suppose that K and L are Witt equivalent. Harrison Theorem asserts that there is an isomorphism of the square-class groups $t : \dot{K}/\dot{K}^2 \to \dot{L}/\dot{L}^2$ such that $t(-1) = -1$ and $1 \in D_K\langle a, b\rangle$ if and only if $1 \in D_L\langle ta, tb\rangle$. It follows that for any $a \in \dot{K}/\dot{K}^2$ we have $ta = \operatorname{disc}\langle 1, -ta\rangle = \operatorname{disc} i_t\langle 1, -a\rangle$.

At the end of Section 1.2 we observed that there is a bijection between the space of orderings of a field and the set o prime ideals of characteristic zero of its Witt ring. Denote it λ_K (respectively λ_L). We know that

$$\lambda_K(\beta) := \ker \operatorname{sgn}_\beta = \bigl\{\xi \in WK : \operatorname{sgn}_\beta \xi = 0\bigr\}.$$

Take now T to be the composition $T := \lambda_L^{-1} \circ \mathbf{i}_t \circ \lambda_K$. Here, $\mathbf{i}_K$ denotes the bijection $\operatorname{Spec} WK \to \operatorname{Spec} WL$ induced by the isomorphism $i_t : WK \to WL$.

We claim that (t, T) is an $\mathcal{X}$-equivalence. Take any square-class $a \in \dot{K}/\dot{K}^2$ and an ordering $\beta \in \mathcal{X}_K$. Suppose that $a \in \beta$, that is $\langle 1, -a\rangle \in \ker \operatorname{sgn}_\beta$. Consequently, $\langle 1, -ta\rangle = i_t\langle 1, -a\rangle \in \mathbf{i}_t \ker \operatorname{sgn}_\beta = \ker \operatorname{sgn}_{T\beta}$. Thus, $ta \in T\beta$ as desired.

Finally, we show that T is continuous. Recall that the Harrison topology of the space of orderings $\mathcal{X}_K$ is generated by a subbasis $\{H(a) : a \in \dot{K}/\dot{K}^2\}$ where $H(a) = \{\beta \in \mathcal{X}_K : a \in \beta\}$. Take any $b \in \dot{L}/\dot{L}^2$ and let $a := t^{-1}(b) \in \dot{K}/\dot{K}^2$. Now

$$T^{-1}\bigl(H(b)\bigr) = \bigl\{\beta \in \mathcal{X}_K : T(\beta) \in H(b)\bigr\} = \bigl\{\beta \in \mathcal{X}_K : ta \in T(\beta)\bigr\} = H(a).$$

It follows that T is continuous. Analogously one shows that T^{-1} is continuous, as well.

We shall now prove the opposite implication. Let (t, T) be an $\mathcal{X}$-equivalence of K, L. By means of Lemma 5.4, without loss of generality, we can assume that $t(-1) = -1$. We claim that t satisfies the assumptions of Harrison Theorem. Take any $a, b \in \dot{K}/\dot{K}^2$ and suppose that the form $\langle a, b\rangle$ represents 1 over K. This means that the 2-fold Pfister form $\langle\langle -a, -b\rangle\rangle$ is hyperbolic. Consequently, for every ordering $\beta \in \mathcal{X}_K$ we have $\operatorname{sgn}_\beta \langle\langle -a, -b\rangle\rangle = 0$. Therefore, for every ordering $\beta' \in \mathcal{X}_L$ one has $\operatorname{sgn}_{\beta'} \langle\langle -ta, -tb\rangle\rangle = 0$. That is, $\langle\langle -ta, -tb\rangle\rangle$ belongs to the kernel of the total signature of L. Now, Pfister's local-global principle (see Theorem 1.37) asserts that $2^r\langle\langle -ta, -tb\rangle\rangle$ is hyperbolic for some $r \in \mathbb{N}_0$. By the assumptions of the theorem, $u(L) \leq 2$, hence $r = 0$ and so $\langle\langle -ta, -tb\rangle\rangle$ is hyperbolic. Consequently, $\langle ta, tb\rangle$ represents 1 over L.

Conversely, suppose that $\langle\langle -ta, -tb\rangle\rangle$ represents 1 over L. In a similar manner as above, we show that $2^r\langle\langle -a, -b\rangle\rangle$ is hyperbolic for some $r \in \mathbb{N}_0$. We assumed that also $u(K) \leq 2$, therefore $\langle\langle -a, -b\rangle\rangle$ is hyperbolic, hence $1 \in D_K\langle a, b\rangle$. □

5.2. Witt equivalence of real holomorphy rings

In this section we concentrate on the subrings of the fields K, L of a special kind, so called the *real holomorphy rings* (see Definition 5.8 below). We show that if both holomorphy rings $\mathcal{H}_K$, $\mathcal{H}_L$ are Dedekind domains and K, L are *tamely* $\mathcal{X}$-equivalent, then the associated strong isomorphism $i_t : WK \to WL$ preserves the Witt rings of their holomorphy rings. We begin with the following lemma, which may be treated as a certain analogy of Witt theorem (compare Theorem 1.55). This is however much simpler then the original one, since the hard part of Witt theorem expressed this way, would be to show that the u-invariant of an algebraic function field of one variable over the real closed field is two.

LEMMA 5.5. *Let K be a formally real field with $u(K) \leq 2$ and let ξ be a quadratic form over K. If* $\operatorname{disc}\xi = 1$ *and* $\operatorname{sgn}_\beta \xi = 0$ *for every ordering $\beta \in \mathcal{X}_K$, then ξ is hyperbolic.*

Proof. By Pfister's local-global principle, the Witt class of ξ belongs to the nilradical $\operatorname{Nil} WK$. Decomposing ξ and knocking-out the hyperbolic part, the anisotropic part of ξ is at most two-dimensional, since $u(K) \leq 2$ by the assumption. It cannot be a unary form as $0 \equiv \operatorname{sgn}_\beta \equiv \dim \xi \pmod 2$. Hence, the anisotropic part is $\langle x, -dx\rangle$ for some $x \in \dot{K}/\dot{K}^2$ and $d = \operatorname{disc}\xi$. But $d = 1$ by the assumption and so ξ is hyperbolic. □

COROLLARY 5.6. *Let K be a formally real field with $u(K) \leq 2$ and let ξ, ζ be two quadratic forms such that*

$$\operatorname{disc}\xi = \operatorname{disc}\zeta \qquad \text{and} \qquad \forall_{\beta\in\mathcal{X}_K} \operatorname{sgn}_\beta \xi = \operatorname{sgn}_\beta \zeta,$$

then the Witt classes of ξ and ζ are equal.

LEMMA 5.7. *Let K be a formally real field, $(\mathcal{O}_\mathfrak{p}, \mathfrak{p})$ a fixed residually real valuation ring of K together with the associated valuation* $\operatorname{ord}_\mathfrak{p}$ *which we assume to be discrete of rank one. Farther, let $\beta_1, \beta_2 \in \mathcal{X}_K$ be any two orderings of K compatible with $\mathfrak{p}$ and pushing down to the same ordering $\overline{\beta}$ of the residue field $K(\mathfrak{p})$. Then for an element $x \in K$, the valuation* $\operatorname{ord}_\mathfrak{p} x$ *is even if and only if x has the same signature in both β_1 and β_2.*

Proof. By Baer-Krull Theorem (see Corollary 1.33), β_1 and β_2 are the only two orderings of K that push down to $\overline{\beta}$. They can both be extended to $K_\mathfrak{p}$ by Corollary 1.30, but $\overline{\beta}$ can be lifted to $K_\mathfrak{p}$ in exactly two ways: by taking a fixed uniformizer to be either positive or negative. Hence, for any $x \in K$ with $\operatorname{ord}_\mathfrak{p} \equiv 1 \pmod 2$ we have $x \in (\beta_1 \setminus \beta_2) \cup (\beta_2 \setminus \beta_1)$. Conversely, let $\operatorname{ord}_\mathfrak{p} x \equiv 0 \pmod 2$. Write $x = p^{2k}u$ for a fixed uniformizer p and some $\mathfrak{p}$-unit u. Then, clearly, $p^{2k} \in \beta_1 \cap \beta_2$ and $u \in \beta_1$ if and only if $\overline{u} \in \overline{\beta_1} = \overline{\beta} = \overline{\beta_2}$ if and only if $u \in \beta_2$. Hence either $x \in \beta_1 \cap \beta_2$ or $-x \in \beta_1 \cap \beta_2$. □

DEFINITION 5.8. The *real holomorphy ring* $\mathcal{H}_K$ of a field K is the intersection of all the residually real valuation rings of K:

$$\mathcal{H}_K := \bigcap_{\substack{\mathfrak{p} \text{ residually} \\ \text{real}}} \mathcal{O}_\mathfrak{p}.$$

We know that for a formally real field K, one has $\operatorname{Nil} WK = \operatorname{Tor} WK$ (see Proposition 1.38). The same remains true for a Dedekind domain since its Witt ring injects into the Witt ring of its field of fractions.

OBSERVATION 5.9. *If the real holomorphy ring $\mathcal{H}_K$ of a real field K is a Dedekind domain, then*

$$\operatorname{Nil} W\mathcal{H}_K = \operatorname{Tor} W\mathcal{H}_K.$$

In fact, the above observation is true also without the assumption that $\mathcal{H}_K$ is Dedekind, due to [20, Theorem 11.1.1]. We will, however, keep the assumption that $\mathcal{H}_K$ is Dedekind since it is needed later anyway. As an explicit example take the ring R of regular functions on a real curve over $\mathbb{R}$ (which we encountered in Chapter 4). It is a real holomorphy ring of the field of rational functions of this curve. Observe that non-zero primes of a real holomorphy ring, that are residually real, are just all the real valuation rings of its field of fractions. Recall that with a given Dedekind domain (in this case $\mathcal{H}_K$) we associate a group $\mathbb{E}(\mathcal{H}_K)$, which can thus be written as:

$$\mathbb{E}(\mathcal{H}_K) := \bigl\{x \in \dot{K}/\dot{K}^2 : \operatorname{ord}_{\mathfrak{p}} x \equiv 0 \pmod 2 \text{ for every residually real } \mathfrak{p}\bigr\}.$$

LEMMA 5.10. *If the real holomorphy ring $\mathcal{H}_K$ of a real field K with $u(K) \le 2$ is a Dedekind domain, then*

$$\operatorname{Nil} W\mathcal{H}_K = \bigl\{\langle 1, -a\rangle : a \in \textstyle\sum \dot{K}^2\bigr\}.$$

Proof. Denote the set on the right hand side by S. We must show two inclusions. First take a totally positive element $a \in \sum \dot{K}^2$. It follows from Lemma 5.7 that $a \in \mathbb{E}(\mathcal{H}_K)$ and so $\langle a\rangle \in W\mathcal{H}_K$ by Corollary 1.46. Consequently $\langle 1, -a\rangle \in W\mathcal{H}_K$. Moreover $\operatorname{sgn}_\beta\langle 1, -a\rangle = 0$ for every ordering $\beta \in \mathcal{X}_K$. Therefore, $\langle 1, -a\rangle \in \operatorname{Nil} WK$ by Pfister local-global principle. All in all, $S \subseteq \operatorname{Nil} W\mathcal{H}_K = W\mathcal{H}_K \cap \operatorname{Nil} WK$.

In order to show the other inclusion, take any non-zero $\xi \in \operatorname{Nil} W\mathcal{H}_K \subset \operatorname{Nil} WK$. By the assumption $u(K) \le 2$, in the Witt class ξ we may find a binary form $\langle a, b\rangle$ for some $a, b \in \dot{K}/\dot{K}^2$. Let d be the discriminant of ξ. Since ξ is a torsion element of the Witt ring, it follows from the Pfister local-global principle, that $\operatorname{sgn}_\beta a = -\operatorname{sgn}_\beta b$ for every ordering $\beta \in \mathcal{X}_K$. Consequently, d is totally positive. Now, the forms $\langle a, b\rangle$ and $\langle 1, -d\rangle$ have the same discriminants and equal signatures with respect to every ordering of K. Corollary 5.6 asserts that they both belong to the same Witt class ξ. □

We need the following result by H.-W. Schülting:

PROPOSITION 5.11 ([49, Corollary 4.7]). *If $\mathcal{H}$ is a real holomorphy ring, then for every $\xi \in W\mathcal{H}$ there are $u_1 \dots, u_n \in U\mathcal{H}$ and $\zeta \in \operatorname{Tor} W\mathcal{H}$ such that*

$$\xi = \zeta + \langle u_1, \dots, u_n\rangle.$$

In particular the reduced Witt ring $W_{red}\mathcal{H}$ is generated by classes of unary forms.

In the previous section we proved that two formally real fields K, L are Witt equivalent if and only if they are $\mathcal{X}$-equivalent. Now, once $\mathcal{H}_K$ and $\mathcal{H}_L$ are Dedekind domains, then $W\mathcal{H}_K$ and $W\mathcal{H}_L$ may be treated as subrings of WK and WL respectively. It is natural to ask, if the isomorphism of Witt rings associated with a given $\mathcal{X}$-equivalence (t, T) preserves this subrings. In general it is not true. However, we can achieve the desired effect by refining the notion of $\mathcal{X}$-equivalence.

Definition 5.12. Suppose that $\mathcal{H}_K$, $\mathcal{H}_L$ are Dedekind domains. We shall say that an $\mathcal{X}$-equivalence (t,T) of the fields K, L is *tame* if the following two conditions are satisfied:

1. if β_1, β_2 are two orderings compatible with the same real valuation, then so are $T\beta_1$ and $T\beta_2$;
2. if the above is the case, then both β_1, β_2 push down to the same ordering of the residue field if and only if $T\beta_1$ and $T\beta_2$ push down to the same ordering.

Observe that the first condition of tame $\mathcal{X}$-equivalence means that T induces a bijection between the sets of all the residually real valuation rings of K and L.

Remark 5.13. The notion of tame $\mathcal{X}$-equivalence is a natural generalization of the notion of tame quaternion-symbol equivalence used in [24, 27, 29]. Note, however, that in the case of a quaternion symbol equivalence of two formally real function fields the residue fields were always real closed. In particular every such a field had the unique ordering and so we didn't need any counterpart for the second condition of the above definition, since it would be trivial anyway. On the other hand, for a general case discussed here we need it right in its place.

Lemma 5.14. *Let K, L be two formally real fields with* $\max\{u(K), u(L)\} \leq 2$ *and assume that their real holomorphy rings are Dedekind. If (t,T) is a tame $\mathcal{X}$-equivalence of K, L, then $t\big(\mathbb{E}(\mathcal{H}_K)\big) = \mathbb{E}(\mathcal{H}_L)$.*

Proof. Fix any $x \in \mathbb{E}(\mathcal{H}_K)$. Lemma 5.7 asserts that for every residually real valuation ring $(\mathcal{O}_\mathfrak{p}, \mathfrak{p})$, every ordering $\overline{\beta}$ of the residue field $K(\mathfrak{p})$ and every two liftings $\beta_1, \beta_2 \in \mathcal{X}_K$ of β one has $x \in \beta_1 \cap \beta_2$. Consequently, $tx \in T\beta_1 \cap T\beta_2$ and—since (t,T) is tame—both $T\beta_1$ and $T\beta_2$ push down to the same ordering in the residue field $L(\mathfrak{q})$, for some residually real valuation ring $(\mathcal{O}_\mathfrak{q}, \mathfrak{q})$ of L. Thus, $\operatorname{ord}_\mathfrak{q} tx$ is even. If $\mathfrak{p}$ ranges now over all the residually real primes of K, then $\mathfrak{q}$ ranges all the residually real primes of L. Consequently $tx \in \mathbb{E}(\mathcal{H}_L)$ and so $t(\mathbb{E}(\mathcal{H}_K)) \subseteq \mathbb{E}(\mathcal{H}_L)$. Substituting (t^{-1}, T^{-1}) for (t,T) one proves the opposite inclusion. $\square$

The following theorem generalizes [27, Proposition 3.4]:

Theorem 5.15. *Let K, L be two real fields with* $\max\{u(K), u(L)\} \leq 2$. *Assume that their real holomorphy rings $\mathcal{H}_K$, $\mathcal{H}_L$ are Dedekind domains. If K, L are tamely $\mathcal{X}$-equivalent, then there is an isomorphism of their Witt rings which maps $W\mathcal{H}_K$ onto $W\mathcal{H}_L$. In particular the real holomorphy rings $\mathcal{H}_K$ and $\mathcal{H}_L$ are Witt equivalent.*

Proof. Let (t,T) be a tame $\mathcal{X}$-equivalence, by virtue of Lemma 5.4, without loss of generality we can assume that $t(-1) = -1$. As in proof of Theorem 5.3, it follows that t is a Harrison's isomorphism, hence $i_t : WK \to WL$, $i_t\langle a_1, \ldots, a_n\rangle :=$

$\langle ta_1, \dots, ta_n\rangle$ is an isomorphism of the Witt rings. Take now any $\xi \in W\mathcal{H}_K \subset WK$. Proposition 5.11 asserts that there is $\zeta \in \operatorname{Nil} W\mathcal{H}_K$ and $u_1, \dots, u_n \in U\mathcal{H}_K$ such that
$$\xi = \zeta + \langle u_1, \dots, u_n\rangle.$$
Now t maps totally positive elements of K onto totally positive elements of L. It follows from Lemma 5.10 that $i_t \operatorname{Nil} W\mathcal{H}_K = \operatorname{Nil} W\mathcal{H}_L$. Likewise, Lemma 5.7 and Lemma 5.14 show that $tu_1, \dots, tu_n \in U\mathcal{H}_L$. Thus
$$i_t\xi = i_t\zeta + \langle tu_1, \dots, t_un\rangle \in \operatorname{Nil} W\mathcal{H}_L + W\mathcal{H}_L \subset W\mathcal{H}_L.$$
Consequently, $i_t(W\mathcal{H}_K) \subseteq W\mathcal{H}_L$. The opposite inclusion follows from the symmetry of assumptions. □

Unfortunately, the previous theorem provides only a sufficient condition but not a necessary one as it can be observed by the following example. Let $K = L = \mathbb{R}(X)$ be the field of rational functions over the reals. Then the space $\mathcal{X}$ of orderings is a double cover of a projective line. Namely with every point $x \in \mathbb{P}^1\mathbb{R}$ we associate the two orderings $\beta_+(x)$ and $\beta_-(x)$ as it was explained in Section 1.4. Define $T : \mathcal{X} \to \mathcal{X}$ by the set of conditions:
$$\begin{aligned}
T\big(\beta_\pm(x)\big) &:= \beta_\pm(x) && \text{if } x \in \mathbb{R} \setminus [-1, 1] \cup \{\infty\}\\
T\big(\beta_\pm(x)\big) &:= \beta_\mp(-x) && \text{if } x \in (-1, 1)\\
T\big(\beta_-(-1)\big) &:= \beta_-(-1) && T\big(\beta_+(-1)\big) := \beta_-(1)\\
T\big(\beta_-(1)\big) &:= \beta_+(-1) && T\big(\beta_+(1)\big) := \beta_+(1).
\end{aligned}$$
Now, treat the square class group $\dot{\mathbb{R}(X)}/\dot{\mathbb{R}}(X)^2$ as a $\mathbb{F}_2$-linear space and decompose it into
$$\dot{\mathbb{R}(X)}/\dot{\mathbb{R}}(X)^2 = \{-1\} \oplus \{\text{sums of squares}\} \oplus V,$$
with V being a subspace with a basis $\big\{(X - a) : a \in \mathbb{R}\big\}$. Take an automorphism t of $\dot{\mathbb{R}(X)}/\dot{\mathbb{R}}(X)^2$ to be the identity on -1 and sums of squares and define it on the basis of V as
$$t(X - a) := \begin{cases} X - a, & \text{if } a \in (-\infty, -1] \cup [1, \infty),\\ (X - a)(X + a)(X + 1), & \text{if } a \in (-1, 1).\end{cases}$$
It is straightforward to check that (t, T) is an $\mathcal{X}$-equivalence. It is not tame, nevertheless the associated strong automorphism of $W\mathbb{R}(X)$ preserves the Witt ring of the real holomorphy rings. On the other hand the following result due to E. Becker and D. Gondard provides us with an immediate necessary condition:

Proposition 5.16 ([4, Corollary 1.4]). *The space of real places of K consists of finitely many connected components $M_1, \dots, M_N$ if and only if the subgroup $U(\mathcal{H}_K) \cap \sum \dot{K}^2$ has a finite index s in the group of units of $\mathcal{H}_K$. If this is the case, then $s = 2^N$.*

Corollary 5.17. *If $\mathcal{H}_K$ and $\mathcal{H}_L$ are Witt equivalent and the associated spaces of real places of K and L consist of finitely many connected components, then the number of components in both spaces are equal.*

In the case of real algebraic curves, it is known (see Theorem 5.24 below), that the number of semi-algebraically connected components is the only invariant of Witt equivalence of the rings of regular functions. It is not clear if this holds in the general context.

Appendix: Quaternion-symbol equivalence of geometric rings

The results presented in the previous two sections are rather of general nature but, as we have already seen earlier in these notes, by narrowing our attention just to function fields over real curves, we can usually say more because we have then a vast amount of geometric tools at our disposal. Therefore, in this appendix we shortly summarize main results obtained in [24, 25, 27, 29]. Chronologically, the geometric case presented here, preceded the general case discussed in the previous two sections.

Again, as in Chapter 4, let $\Bbbk$ be a fixed real closed field, K and L are two algebraic function fields of one variable over $\Bbbk$, γ_K, γ_L are the associated real curves and R_K, R_L are the rings of regular functions on γ_K and γ_L respectively. It is worth to stress the point that R_K (resp. R_L) is the real holomorphy ring $\mathcal{H}_K$ (resp. $\mathcal{H}_L$) introduced in the previous section if $\Bbbk$ is Archimedean. Otherwise, $\mathcal{H}_K$ is a subring of R_K. The point is, that we obtain the ring R_K by considering all the real valuations that are trivial on the field of constants $\Bbbk$. On the other hand, in case of $\mathcal{H}_K$ we intersect *all* the residually real valuation rings of K. This is precisely the reason why, in what follows, we always consider the semi-algebraically connected components of γ_K and not just the connected components. Of course, if $\Bbbk = \mathbb{R}$ these two notions coincide.

First let us dispose of the special case when the fields in question are non-real.

Proposition 5.18 ([24, Proposition 2.2]). *Let K be a non-real algebraic function field with real closed field of constants $\Bbbk$. Then K is Witt equivalent to $\Bbbk(X)\big(\sqrt{-(X^2+1)}\big)$.*

Corollary 5.19. *Every two non-real algebraic function fields over a common real closed field of constants are Witt equivalent.*

From now on, we shall assume that both K and L are formally real. The main tool used to investigate Witt equivalence of function fields is the notion of quaternion symbol equivalence introduced in [24].

Definition 5.20. Let $A \subseteq \gamma(K)$ and $B \subseteq \gamma(L)$ be subsets of the sets of real points of two function fields K and L. We say that the function fields K and L are *quaternion-symbol equivalent* with respect to the sets A and B when there exists a pair of maps (t,T) in which $t : \dot K/\dot K^2 \to \dot L/\dot L^2$ is an isomorphism of square-class groups, and $T : A \to B$ is a bijection preserving the splitting of local quaternion symbols in the sense that

$$\left(\frac{f,g}{K_{\mathfrak p}}\right) = 1 \in \operatorname{Br} K \iff \left(\frac{tf,tg}{L_{T\mathfrak p}}\right) = 1 \in \operatorname{Br} L \tag{5.1}$$

for all square classes $f,g \in \dot K/\dot K^2$ and all points $\mathfrak p \in A$.

The reader may wish to compare this definition with the definition of an $\mathcal X$-equivalence. As in the case of an $\mathcal X$-equivalence, the isomorphism t does not have to preserve -1. Nevertheless, if (t,T) is a quaternion-symbol equivalence with respect to *big enough* sets A, B (a set is big enough if it contains all but finitely many real points), then there is another one that maps -1 to -1. The proof is nearly identical to the proof of Lemma 5.4 (see [24, Proposition 2.6]). Further, we always assume that $t(-1) = -1$.

Proposition 5.21. *If $S_K \subset \gamma_K$, $S_L \subset \gamma_L$ are two finite (possibly empty) sets and (t,T) is a quaternion-symbol equivalence of K, L with respect to $(\gamma_K \setminus S_K, \gamma_L \setminus S_L)$, then*

1. *$T : (\gamma_K \setminus S_K) \to (\gamma_L \setminus S_L)$ is a homeomorphism;*
2. *for every $\mathfrak p \in \gamma_K \setminus S_K$ and every $x \in \dot K/\dot K^2$ one has $\operatorname{ord}_{\mathfrak p} x$ is even if and only if $\operatorname{ord}_{T\mathfrak p} tx$ is even;*
3. *for every $\mathfrak p \in \gamma_K \setminus S_K$, t maps the fan of orderings compatible with $\mathfrak p$ onto the fan of orderings compatible with $T\mathfrak p$.*

The proof of this proposition follows from [24, Lemmas 3.3, 3.6, 4.1] and [25, Theorem 3.1]. It turns out that not only every quaternion-symbol equivalence incorporates a homeomorphism, but also with every homeomorphism one can associate a quaternion-symbol equivalence. What's more, every quaternion-symbol equivalence gives rise to Witt equivalence et vice versa. The reader may wish to compare the following proposition with Theorem 5.3.

Proposition 5.22. *The following conditions are equivalent:*

1. *there is a homeomorphism $T : (\gamma_K \setminus S_K) \to (\gamma_L \setminus S_L)$ for some finite (possibly empty) sets S_K, S_L;*
2. *there is a quaternion-symbol equivalence (t,T) with respect to $(\gamma_K \setminus S_K, \gamma_L \setminus S_L)$ of the fields K, L for some finite (possibly empty) sets S_K, S_L;*
3. *fields K and L are Witt equivalent.*

For the proof see [24, Lemma 4.1 and Corollary 4.2]. Now, every component of a real curve is homeomorphic to a projective line $\mathbb P^1\Bbbk$ and every open interval is homeomorphic to a unit interval $(0,1) \subset \Bbbk$. Suppose that γ_K consists of N and γ_L of M semi-algebraically connected components. If $N = M$ then γ_K and γ_L are homeomorphic. Otherwise, suppose that $N < M$ and knock-out $M - N + 1$ distinct points $\mathfrak{p}_1, \dots, \mathfrak{p}_{M-N+1}$ from *one* of the components of γ_K, splitting it into $M-N+1$ disjoint open intervals. Next, remove $\mathfrak{q}_1, \dots, \mathfrak{q}_{M-N+1}$ points from *distinct* components of γ_L. This "converts" $M - N + 1$ components of γ_L to open intervals. Now, pairing the open intervals with open intervals and the remaining components of γ_K with remaining components of γ_L, we see that $\gamma_K \setminus \{\mathfrak{p}_1 \dots, \mathfrak{p}_{M-N+1}\}$ is homeomorphic to $\gamma_L \setminus \{\mathfrak{q}_1, \dots, \mathfrak{q}_{M-N+1}\}$. It follows from the above proposition that K, L are Witt equivalents. Combining this with Corollary 5.19 we get (see also [19, Corollary 3.6]):

THEOREM 5.23 ([24, Theorem 5.1]). *Two algebraic function fields with a common real closed field of constants are Witt equivalent if and only if they are both real or both non-real.*

This is by no means the end of the story. It occurs that if we can construct a quaternion-sumbol equivalence with respect to the whole sets γ_K, γ_L of real points, which by Proposition 5.21 is possible when γ_K and γ_L consists of the same number of semialgebraically connected components, then the isomorphism t maps $\mathbb{E}(R_K)$ onto $\mathbb{E}(R_L)$. This leads to Witt equivalence of the rings of regular functions:

THEOREM 5.24 ([29, Corollary 4.2]). *The following conditions are equivalent:*

1. *the rings R_K, R_L are Witt equivalent;*
2. *the real curves γ_K, γ_L consists of the same number of semi-algebraically connected components;*
3. *the Knebusch-Milnor exact sequences associated with R_K and R_L are isomorphic.*

It is worth to stress the point that Witt equivalence of rings of regular functions on two real curves depends solely on the number of semi-algebraically connected components of these two curves and not on the relative position of these components, neither directly on degrees of these curves nor on their genuses. To see this phenomenon clearly consider two curves (illustrated in Fig. 5.1) defined by the following polynomials (found using [38]):

$$\begin{aligned} C_0 &= \big(y^2 + x(x+1)\big)\big(x^2 + y^2\big) - \frac{x^2 + y^2 - 2}{100} - 4xy^2 \\ C_1 &= \big(y^2 + x^2 - 9\big)\Big(\frac{y^2 + x^4 - 16}{20} + \big(y^2 + x^2 - 4\big)\big(y^2 + x^2 - 1\big)\Big) \\ &\qquad + \frac{y^2 + x^4 - 25}{100} \end{aligned} \tag{5.2}$$

Both curves consist of three components, hence Theorem 5.24 asserts that the rings of regular functions on these two curves are Witt equivalent. On the other hand, the configuration of the components of the first curve is $1 \amalg 1 \amalg 1$ while the second curve has a configuration $1\langle 1\langle 1\rangle\rangle$. Likewise, the degrees of the two curves differ:

$$\deg C_0 = 4 \neq 6 = \deg C_1.$$

Finally, since both curves are smooth and their degrees differ by more than one, the genuses of these two curves are different, as well.

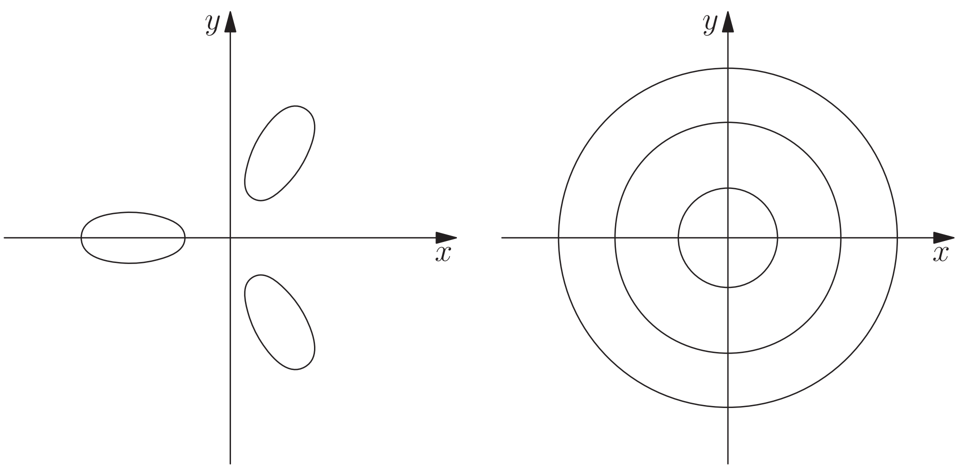


Figure 5.1. Curves with Witt equivalent rings of regular functions defined by Eq. (5.2)

Bibliography

[1] Michael F. Atiyah and Ian. G. Macdonald: *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.–London–Don Mills, Ont., 1969.

[2] Ricardo Baeza: *Quadratic forms over semilocal rings*, *Lecture Notes in Mathematics*. Vol. 655. Springer-Verlag, Berlin, 1978.

[3] Hyman Bass: *Algebraic K-theory*. W.A. Benjamin, Inc., New York–Amsterdam, 1968.

[4] Eberhard Becker: The real holomorphy ring and sums of $2n$th powers. In: *Real algebraic geometry and quadratic forms (Rennes, 1981)*. Vol. 959 of *Lecture Notes in Math.*. Springer, Berlin, 1982, p. 139–181.

[5] Jacek Bochnak, Michel Coste and Marie-Françoise Roy: *Real algebraic geometry*. Vol. 36 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1998.

[6] Nicolas Bourbaki: *Elements of mathematics. Commutative algebra*. Hermann, Paris, 1972. Translated from the French.

[7] Egbert Brieskorn and Horst Knörrer: *Plane algebraic curves*. Birkhäuser Verlag, Basel, 1986. Translated from the German by John Stillwell.

[8] Winfried Bruns and Joseph Gubeladze: *Polytopes, rings, and K-theory*. Springer Monographs in Mathematics. Springer, Dordrecht, 2009.

[9] Andrew B. Carson and Murray A. Marshall: Decomposition of Witt rings. *Canad. J. Math.*, 34(6): 1276–1302, 1982.

[10] Marzena Ciemała: Natural homomorphisms of Witt rings of orders in algebraic number fields. II. *Acta Math. Univ. Ostrav.*, 14(1): 13–16, 2006.

[11] Marzena Ciemała and Kazimierz Szymiczek: On the existence of nonsingular bilinear forms on projective modules. *Tatra Mt. Math. Publ.*, 32: 1–13, 2005.

[12] Marzena Ciemała and Kazimierz Szymiczek: On injectivity of natural homomorphisms of Witt rings. *Ann. Math. Sil.*, (21): 15–30 (2008), 2007.

[13] Thomas C. Craven, Alex Rosenberg, and Roger Ware: The map of the Witt ring of a domain into the Witt ring of its field of fractions. *Proc. Amer. Math. Soc.*, 51: 25–30, 1975.

[14] Hans Delfs and Manfred Knebusch: Semialgebraic topology over a real closed field. I. Paths and components in the set of rational points of an algebraic variety. *Math. Z.*, 177(1): 107–129, 1981.

[15] David Eisenbud: *Commutative Algebra : with a View Toward Algebraic Geometry (Graduate Texts in Mathematics)*. Springer, February 1999.

[16] Richard Elman, Tsit Yuen Lam and Alexander Prestel: On some Hasse principles over formally real fields. *Math. Z.*, 134: 291–301, 1973.

[17] Otto Endler: *Valuation theory*. Springer-Verlag, New York, 1972.

[18] Daniel R. Grayson and Michael E. Stillman: Macaulay2, a software system for research in algebraic geometry. Available at `http://www.math.uiuc.edu/Macaulay2`.

[19] Nicolas Grenier-Boley and Detlev Hoffmann: Isomorphism criteria for witt rings of real fields. *Forum Mathematicum*, 2011.

[20] Manfred Knebusch: Grothendieck- und Wittringe von nichtausgearteten symmetrischen Bilinearformen. *S.-B. Heidelberger Akad. Wiss. Math.-Natur. Kl.*, 1969/70: 93–157, 1969/1970.

[21] Manfred Knebusch: On algebraic curves over real closed fields. I. *Math. Z.*, 150(1): 49–70, 1976.

[22] Manfred Knebusch: On algebraic curves over real closed fields. II. *Math. Z.*, 151(2): 189–205, 1976.

[23] Przemysław Koprowski: Local-global principle for Witt equivalence of function fields over global fields. *Colloq. Math.*, 91(2): 293–302, 2002.

[24] Przemysław Koprowski: Witt equivalence of algebraic function fields over real closed fields. *Math. Z.*, 242(2): 323–345, 2002.

[25] Przemysław Koprowski: Integral equivalence of real algebraic function fields. *Tatra Mt. Math. Publ.*, 32: 53–61, 2005.

[26] Przemysław Koprowski: On splitting the Knebusch-Milnor exact sequence. *J. Algebra*, 301(2): 616–626, 2006.

[27] Przemysław Koprowski: On existence of tame Harrison map. *Math. Slovaca*, 57(5): 407–414, 2007.

[28] Przemysław Koprowski: Splitting natural injection of Witt rings of geometric rings. *Int. J. Pure Appl. Math.*, 45(1): 5–11, 2008.

[29] Przemysław Koprowski: Witt equivalence of rings of regular functions. *Ann. Math. Sil.*, (22): 45–57 (2009), 2008.

[30] Ernst Kunz: *Introduction to commutative algebra and algebraic geometry*. Birkhäuser Boston Inc., Boston, MA, 1985. Translated from the German by Michael Ackerman, With a preface by David Mumford.

[31] Tsit Yuen Lam: *Orderings, valuations and quadratic forms*. Vol. 52 of *CBMS Regional Conference Series in Mathematics*. Published for the Conference Board of the Mathematical Sciences, Washington, DC, 1983.

[32] Tsit Yuen Lam: *Lectures on modules and rings*. Vol. 189 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1999.

[33] Tsit Yuen Lam: *Introduction to quadratic forms over fields*. Vol. 67 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2005.

[34] Serge Lang: *Algebra*. Vol. 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[35] Henri Lombardi and Claude Quitté: Comparison of Picard groups in dimension 1. *MLQ Math. Log. Q.*, 54(3): 247–252, 2008.

[36] Murray A. Marshall: *Bilinear forms and orderings on commutative rings*. Vol. 71 of *Queen's Papers in Pure and Applied Mathematics*. Queen's University, Kingston, ON, 1985.

[37] Murray A. Marshall: *Spaces of orderings and abstract real spectra*. Vol. 1636 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1996.

[38] Maxima, a computer algebra system version 5.19.2. Available at `http://maxima.sourceforge.net`, 2010.

[39] John Milnor and Dale Husemoller: *Symmetric bilinear forms*. Springer-Verlag, New York, 1973.

[40] Jean-Philippe Monnier: Witt group and torsion Picard group of real curves. *J. Pure Appl. Algebra*, 169(2–3): 267–293, 2002.

[41] O. Timothy O'Meara: *Introduction to quadratic forms*. Classics in Mathematics. Springer-Verlag, Berlin, 2000. Reprint of the 1973 edition.

[42] I. Panin and U. Rehmann: A variant of a theorem by Springer. *Algebra i Analiz*, 19(6): 117–125, 2007.

[43] Raman Parimala and Raja Sridharan: Quadratic forms over rings of dimension 1. *Comment. Math. Helv.*, 55(4): 634–644, 1980.

[44] Rober Perlis, Kazimierz Szymiczek, Pierre E. Conner, and Richard Litherland: Matching Witts with global fields. In: *Recent advances in real algebraic geometry and quadratic forms (Berkeley, CA, 1990/1991; San Francisco, CA, 1991)*. Vol. 155 of *Contemp. Math.*. Amer. Math. Soc., Providence, RI, 1994, p. 365–387.

[45] Beata Rothkegel: Nonsingular bilinear forms on a direct sum of ideals. preprint, 2011.

[46] Beata Rothkegel and Alfred Czogała: Witt equivalence of semilocal Dedekind domains in global fields. *Abh. Math. Sem. Univ. Hamburg*, 77: 1–24, 2007.

[47] Beata Rothkegel and Alfred Czogała: Singular elements and the Witt equivalence of rings of algebraic integers. *Ramanujan J.*, 17(2): 185–217, 2008.

[48] Louis H. Rowen: *Ring theory. I.* Vol. 127 of *Pure and Applied Mathematics.* Academic Press Inc., Boston, MA, 1988.

[49] Heinz-Werner Schülting: On real places of a field and their holomorphy ring. *Comm. Algebra*, 10(12): 1239–1284, 1982.

[50] Parvati Shastri: Witt groups of algebraic integers. *J. Number Theory*, 30(3): 243–266, 1988.

[51] Henning Stichtenoth: *Algebraic function fields and codes.* Universitext. Springer-Verlag, Berlin, 1993.

[52] Kazimierz Szymiczek: Matching Witts locally and globally. *Math. Slovaca*, 41(3): 315–330, 1991.

[53] Kazimierz Szymiczek: Witt equivalence of global fields. *Comm. Algebra*, 19(4): 1125–1149, 1991.

[54] Kazimierz Szymiczek: *Bilinear algebra.* Vol. 7 of *Algebra, Logic and Applications.* Gordon and Breach Science Publishers, Amsterdam, 1997. An introduction to the algebraic theory of quadratic forms.

[55] Kazimierz Szymiczek: Witt ring of a commutative ring. Talk at the ANTh Seminar, 2002.

[56] Carlo Traverso: Seminormality and Picard group. *Ann. Scuola Norm. Sup. Pisa (3)*, 24: 585–595, 1970.

[57] Ch. Weibel: An introduction to algebraic K-theory. Online notes. Available at `http://www.math.uiuc.edu/K-theory/0105`,

[58] K. Zainoulline: On Knebusch's norm principle for quadratic forms over semi-local rings. *Math. Z.*, 251(2): 415–425, 2005.

Commonly used symbols

$\rightarrowtail$	— injection/monomorphism
$\xrightarrow{\sim}$	— bijection/isomorphism
$\twoheadrightarrow$	— surjection/epimorphism
$\langle u_1, \dots, u_k \rangle$	— diagonal form (see p. 13)
$\langle\langle u_1, \dots, u_k \rangle\rangle$	— Pfister form (see p. 13)
$\left(\frac{a,b}{K}\right)$	— quaternion algebra over K
Θ_V	— null vector of a vector space V
$\mathbb{A}^n K$	— n-dimensional affine K-space
ann	— annihilator
Br	— Brauer group/functor
$\mathfrak{c}$	— conductor of a ring extension
$\chi_{(\mathfrak{p},\mathfrak{q})}$	— interval function (see p. 26)
$D_K(\xi)$	— set of elements represented by ξ in K
det	— determinant
disc	— discriminant (see p. 13)
∂	— second residue homomorphism (see p. 20)
$\mathbb{E}$	— see p. 23
γ, γ_K	— real algebraic curve
$G_P(\xi)$	— group of similarity factors of ξ (see p. 37)
$H(a)$	— element of a subbasis of Harrison topology (see p. 20)
$\mathcal{H}$	— real holomorphy ring (see p. 76)
$\mathrm{Hom}_P(M, N)$	— module of homomorphism of P-modules M, N
im	— image of a morphism
ker	— kernel of a morphism
$\dot{K}/\dot{K}^2$	— square-class group of K

$\mathbb{N}$	— positive integers
$\mathbb{N}_0$	— non-negative integers
Nil	— nilradical (see p. 19)
$\mathcal{O}, \mathcal{O}_\mathfrak{p}, (\mathcal{O}_\mathfrak{p}, \mathfrak{p})$	— valuation ring
$\Omega, \Omega(K)$	— set of valuation rings if K
$\mathrm{ord}_\mathfrak{p}$	— discrete valuation with a valuation ring $(\mathcal{O}_\mathfrak{p}, \mathfrak{p})$ (see p. 18)
$\dot{P}$	— set of non-zero-divisors of P
Pic	— Picard group/functor
$\mathbb{P}^n K$	— n-dimensional projective K-space
qf	— field of fractions
$\mathbb{Q}$	— field of rationals
Rad	— Jacobson's radical
$\mathbb{R}$	— field of reals
sgn_β	— signature associated with an ordering β
$\mathrm{sgn}_\mathfrak{p}$	— sign at a point $\mathfrak{p}$
Sgn	— total signature
$\sum \dot{P}^2$	— set of sums of squares in P
Spec	— spectrum of a ring
$S^\perp$	— orthogonal completion of S (see p. 12)
s_*	— transfer (see p. 34)
Tor	— set of torsion elements (see p. 19)
UP	— group of units of P
$u(K)$	— u-invariant of K (see p. 74)
WP	— Witt ring/group of P (see p. 15)
$\Xi(\xi, \mathscr{B})$	— matrix of a form ξ in a basis $\mathscr{B}$
$\mathbb{Z}$	— ring of integers

Index

Przemysław Koprowski

Morfizmy pierścieni Witta

S t r e s z c z e n i e

Rozprawa *Witt morphisms* omawia właściwości funktora Witta na kategorii pierścieni przemiennych z jedynką. Książka składa się z pięciu rozdziałów, z których pierwszy ma charakter wprowadzający do tematyki funktora Witta. W rozdziale tym są zdefiniowane kluczowe pojęcia niezbędne do rozumienia dalszych części pracy i przywołane standardowe wyniki używane w kolejnych rozdziałach. Główną część pracy stanowią rozdziały 2–5. Rozdział drugi omawia problematykę zachowania funktora Witta na rozszerzeniach unitarnych (a w szczególności na kwadratowych rozszerzeniach unitarnych) pierścieni lokalnych. Rozdział ten zawiera między innymi uogólnienie techniki transferowej Scharlau'a na przypadek rozszerzeń niewolnych. Rozdział trzeci wykorzystuje wyniki rozdziału poprzedniego do badania zachowania funktora Witta normalizacji dziedzin wymiaru jeden. W rozdziale tym w szczególności poruszana jest kwestia (nie)injektywności funktora Witta normalizacji. Rozdział czwarty poświęcony jest tematyce rozszczepialności ciągu dokładnego Knebuscha–Milnora dla pierścieni geometrycznych. Ostatni, piąty, rozdział rozprawy dotyczy równoważności Witta rzeczywistych ciał i pierścieni, czyli istnienia izomorfizmu między pierścieniami Witta dwóch struktur algebraicznych.

Przemysław Koprowski

Wittmorphismen

Z u s a m m e n f a s s u n g

Das Buch *Witt morphisms* befasst sich mit den Eigenschaften des Wittfunktors in der Kategorie der kommutativen Ringe mit Eins. Das Buch hat fünf Kapitel. Das erste gibt eine Einfuehrung in die Terminologie und die klassischen Resultate, die für die weiteren Kapitel notwendig sind. Die Hauptresultate des Buches sind in den Kapiteln 2–5 enthalten. Das zweite Kapitel diskutiert das Verhalten des Wittfunktors unter unitären Erweiterungen (inbesondere unter quadratischen unitären Erweiterungen) lokaler Ringe. Neben anderen Themen enthaelt dieses Kapitel eine Verallgemeinerung von Scharlaus Transferprinzip für nicht-freie Erweiterungen. Gegenstand des dritten Kapitels ist das Verhalten des Wittfunktors unter Normalisierung. Eines der Hauptthemen ist die Nicht-Injektivität des Wittfunktors unter Normalisierung. Das vierte Kapitel beschäftigt sich mit dem Problem der Zerfällung der Knebusch–Milnor exakten Folge für geometrische Ringe. Das letzte, fünfte Kapitel behandelt die Theorie der Witt-Äquivalenz formal reeller Ringe und Körper.

Redaktor
Barbara Todos-Burny

Redaktor techniczny
Barbara Arenhövel

Projektant okładki, skład i łamanie
Przemysław Koprowski

ISSN 0208-6336
ISBN 978-83-226-2113-4

Wydawca
Wydawnictwo Uniwersytetu Śląskiego
ul. Bankowa 12B, 40-007 Katowice
www.wydawnictwo.us.edu.pl
e-mail: wydawus@us.edu.pl

Wydanie I. Ark. druk. 6,0. Ark. wyd. 7,0.
Papier offset. kl. III, 90 g Cena 8 zł (+ VAT)

Druk i oprawa: PPHU TOTEM s.c.
M. Rejnowski, J. Zamiara
ul. Jacewska 89, 88-100 Inowrocław

Cena 8 zł (+ VAT)

ISSN 0208-6336
ISBN 978-83-226-2113-4